
MySQL 5.0 Release Notes

Abstract

This document contains release notes for the changes in each release of MySQL 5.0, up through MySQL 5.0.96. It describes all enhancements and bug fixes made to MySQL Enterprise Server and MySQL Community Server. For information about changes in a different MySQL series, see the release notes for that series.

End of Product Lifecycle. Active development for MySQL Database Server version 5.0 has ended. Oracle offers various support offerings which may be of interest. For details and more information, see the MySQL section of the Lifetime Support Policy for Oracle Technology Products (<http://www.oracle.com/us/support/lifetime-support/index.html>). Please consider upgrading to a recent version.

For additional MySQL 5.0 documentation, see the [MySQL 5.0 Reference Manual](#), which includes an overview of features added in MySQL 5.0 ([What Is New in MySQL 5.0](#)), and discussion of upgrade issues that you may encounter for upgrades from MySQL 4.1 to MySQL 5.0 ([Changes Affecting Upgrades to 5.0](#)).

Releases in MySQL Enterprise Server are divided into the following types of release packs:

Rapid Update Service Packs are issued once a month and incorporate all the bug fixes and security updates introduced since the previous MySQL Enterprise Server release. A single Service Pack can be used to update MySQL Enterprise Server; it is not necessary to install intervening service packs to bring your system up to date.

Quarterly Service Packs are issued each quarter and incorporate all the bug fixes and security updates introduced up to the Rapid Update that the QSP it is based on, and possibly some critical bug fixes and security updates from later releases. A single Service Pack can be used to update MySQL Enterprise Server; it is not necessary to install intervening service packs to bring your system up to date.

Hot-fix releases incorporate fixes for bugs that caused significant issues that are not released as part of a Service Pack.

For information on how to determine your current version and release type, see [Determining Your Current MySQL Version](#).

For legal information, see the [Legal Notices](#).

For help with using MySQL, please visit either the [MySQL Forums](#) or [MySQL Mailing Lists](#), where you can discuss your issues with other MySQL users.

For additional documentation on MySQL products, including translations of the documentation into other languages, and downloadable versions in variety of formats, including HTML and PDF formats, see the [MySQL Documentation Library](#).

Document generated on: 2016-05-11 (revision: 8866)

Table of Contents

Preface and Legal Notices	3
Changes in MySQL 5.0.96 (2012-03-21)	5
Changes in MySQL 5.0.95 (2012-01-10)	5
Changes in MySQL 5.0.94 (2011-07-05)	5
Changes in MySQL 5.0.93 (2011-05-05)	6
Changes in MySQL 5.0.92 (2011-02-07)	6
Changes in MySQL 5.0.91 (2010-05-05)	8
Changes in MySQL 5.0.90 (2010-01-15)	9
Changes in MySQL 5.0.89 (2009-12-02)	10

Changes in MySQL 5.0.88 (2009-11-04)	11
Changes in MySQL Enterprise 5.0.87sp1 [QSP] (2010-02-03)	12
Changes in MySQL 5.0.87 (2009-10-15)	14
Changes in MySQL 5.0.86 (2009-09-09)	15
Changes in MySQL 5.0.85 (2009-08-11)	16
Changes in MySQL Enterprise 5.0.84sp1 [QSP] (2009-09-30)	17
Changes in MySQL 5.0.84 (2009-07-07)	18
Changes in MySQL 5.0.83 (2009-05-29)	19
Changes in MySQL Enterprise 5.0.82sp1 [QSP] (2009-07-21)	21
Changes in MySQL 5.0.82 (2009-05-20)	21
Changes in MySQL Community Server 5.0.81 (2009-05-01)	23
Changes in MySQL Enterprise 5.0.80 [MRU] (2009-05-01)	27
Changes in MySQL Enterprise 5.0.79 [MRU] (2009-03-09)	29
Changes in MySQL Enterprise 5.0.78 [MRU] (2009-02-06)	31
Changes in MySQL Community Server 5.0.77 (2009-01-28)	33
Changes in MySQL Enterprise 5.0.76 [MRU] (2009-01-05)	40
Changes in MySQL Community Server 5.0.75 (2008-12-17)	42
Changes in MySQL Enterprise 5.0.74sp1 [QSP] (2009-04-30)	48
Changes in MySQL Enterprise 5.0.74 [MRU] (2008-12-03)	49
Changes in MySQL Enterprise 5.0.72sp1 [QSP] (2009-01-13)	50
Changes in MySQL Enterprise 5.0.72 [MRU] (2008-10-24)	51
Changes in MySQL Enterprise 5.0.70 [MRU] (2008-09-27)	53
Changes in MySQL Enterprise 5.0.68 [MRU] (2008-08-13)	55
Changes in MySQL Community Server 5.0.67 (2008-08-04)	56
Changes in MySQL Enterprise 5.0.66sp1 [QSP] (2008-10-23)	80
Changes in MySQL Enterprise 5.0.66a [MRU] (2008-07-16)	81
Changes in MySQL Enterprise 5.0.66 [MRU] (2008-07-09)	81
Changes in MySQL Enterprise 5.0.64 [MRU] (2008-06-10)	82
Changes in MySQL Enterprise 5.0.62 [MRU] (2008-05-12)	83
Changes in MySQL Enterprise 5.0.60sp1 [QSP] (2008-06-27)	84
Changes in MySQL Enterprise 5.0.60 [MRU] (2008-04-28)	85
Changes in MySQL Enterprise 5.0.58 [MRU] (2008-03-05)	90
Changes in MySQL Enterprise 5.0.56sp1 [QSP] (2008-03-30)	93
Changes in MySQL Enterprise 5.0.56 [MRU] (2008-02-06)	106
Changes in MySQL Enterprise 5.0.54a [MRU] (2008-01-11)	109
Changes in MySQL Enterprise 5.0.54 [MRU] (2007-12-14)	110
Changes in MySQL Enterprise 5.0.52 [MRU] (2007-11-30)	115
Changes in MySQL Community Server 5.0.51b (2008-04-24)	121
Changes in MySQL Community Server 5.0.51a (2008-01-11)	122
Changes in MySQL Community Server 5.0.51 (2007-11-15)	122
Changes in MySQL Enterprise 5.0.50sp1a [QSP] (2008-01-11)	134
Changes in MySQL Enterprise 5.0.50sp1 [QSP] (2007-12-12)	135
Changes in MySQL Enterprise 5.0.50 [MRU] (2007-10-19)	135
Changes in MySQL Enterprise 5.0.48 [MRU] (2007-08-27)	138
Changes in MySQL Enterprise 5.0.46 [MRU] (2007-07-13)	144
Changes in MySQL Community Server 5.0.45 (2007-07-04)	148
Changes in MySQL Enterprise 5.0.44sp1 [QSP] (2007-08-01)	159
Changes in MySQL Enterprise 5.0.44 [MRU] (2007-06-21)	159
Changes in MySQL Enterprise 5.0.42 [MRU] (2007-05-23)	165
Changes in MySQL Community Server 5.0.41 (2007-05-01)	170
Changes in MySQL Enterprise 5.0.40 [MRU] (2007-04-17)	180
Changes in MySQL Enterprise 5.0.38 [MRU] (2007-03-20)	186
Changes in MySQL Community Server 5.0.37 (2007-02-27)	191
Changes in MySQL Enterprise 5.0.36sp1 [QSP] (2007-04-12)	199

Changes in MySQL Enterprise 5.0.36 [MRU] (2007-02-20)	199
Changes in MySQL Enterprise 5.0.34 [MRU] (2007-01-17)	205
Changes in MySQL Community Server 5.0.33 (2007-01-09)	207
Changes in MySQL Enterprise 5.0.32 [MRU] (2006-12-20)	218
Changes in MySQL Enterprise 5.0.30sp1 [QSP] (2007-01-19)	223
Changes in MySQL Enterprise 5.0.30 [MRU] (2006-11-14)	224
Changes in MySQL Enterprise 5.0.28 (2006-10-24)	229
Changes in MySQL Community Server 5.0.27 (2006-10-21)	230
Changes in MySQL 5.0.26 (2006-10-03)	230
Changes in MySQL 5.0.25 (2006-09-15)	234
Changes in MySQL 5.0.24a (2006-08-25)	245
Changes in MySQL 5.0.24 (2006-07-27)	246
Changes in MySQL 5.0.23 (Not released)	248
Changes in MySQL 5.0.22 (2006-05-24)	257
Changes in MySQL 5.0.21 (2006-05-02)	258
Changes in MySQL 5.0.20a (2006-04-18)	262
Changes in MySQL 5.0.20 (2006-03-31)	263
Changes in MySQL 5.0.19 (2006-03-04)	267
Changes in MySQL 5.0.18 (2005-12-21)	274
Changes in MySQL 5.0.17 (2005-12-14)	276
Changes in MySQL 5.0.16 (2005-11-10)	281
Changes in MySQL 5.0.15 (2005-10-19, Production)	285
Changes in MySQL 5.0.14 (Not released)	289
Changes in MySQL 5.0.13 (2005-09-22, Release Candidate)	291
Changes in MySQL 5.0.12 (2005-09-02)	296
Changes in MySQL 5.0.11 (2005-08-06)	301
Changes in MySQL 5.0.10 (2005-07-27)	303
Changes in MySQL 5.0.9 (2005-07-15)	307
Changes in MySQL 5.0.8 (Not released)	310
Changes in MySQL 5.0.7 (2005-06-10)	314
Changes in MySQL 5.0.6 (2005-05-26)	318
Changes in MySQL 5.0.5 (Not released)	322
Changes in MySQL 5.0.4 (2005-04-16)	324
Changes in MySQL 5.0.3 (2005-03-23, Beta)	327
Changes in MySQL 5.0.2 (2004-12-01)	337
Changes in MySQL 5.0.1 (2004-07-27)	341
Changes in MySQL 5.0.0 (2003-12-22, Alpha)	345

Preface and Legal Notices

This document contains release notes for the changes in each release of MySQL 5.0, up through MySQL 5.0.96.

End of Product Lifecycle. Active development for MySQL Database Server version 5.0 has ended. Oracle offers various support offerings which may be of interest. For details and more information, see the MySQL section of the Lifetime Support Policy for Oracle Technology Products (<http://www.oracle.com/us/support/lifetime-support/index.html>). Please consider upgrading to a recent version.

Legal Notices

Copyright © 1997, 2016, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted

in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

This documentation is NOT distributed under a GPL license. Use of this documentation is subject to the following terms:

You may create a printed copy of this documentation solely for your own personal use. Conversion to other formats is allowed as long as the actual content is not altered or edited in any way. You shall not publish or distribute this documentation in any form or on any media, except if you distribute the documentation in a manner similar to how Oracle disseminates it (that is, electronically for download on a Web site with the software) or on a CD-ROM or similar medium, provided however that the documentation is disseminated together with the software on the same medium. Any other use, such as any dissemination of printed copies or use of this documentation, in whole or in part, in another publication, requires the prior written consent from an authorized representative of Oracle. Oracle and/or its affiliates reserve any and all rights to this documentation not expressly granted above.

Changes in MySQL 5.0.96 (2012-03-21)

End of Product Lifecycle. Active development for MySQL Database Server version 5.0 has ended. Oracle offers various support offerings which may be of interest. For details and more information, see the MySQL section of the Lifetime Support Policy for Oracle Technology Products (<http://www.oracle.com/us/support/lifetime-support/index.html>). Please consider upgrading to a recent version.

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- yaSSL was upgraded from version 1.7.2 to 2.2.0. (Bug #13706828)

References: See also: Bug #13713205.

Bugs Fixed

- yaSSL fixes previously applied to MySQL 5.5 were backported to 5.0 and 5.1. (Bug #13706621)
- Large values passed to `FORMAT()` caused a buffer overflow and a server exit. (Bug #12406055)

Changes in MySQL 5.0.95 (2012-01-10)

End of Product Lifecycle. Active development for MySQL Database Server version 5.0 has ended. Oracle offers various support offerings which may be of interest. For details and more information, see the MySQL section of the Lifetime Support Policy for Oracle Technology Products (<http://www.oracle.com/us/support/lifetime-support/index.html>). Please consider upgrading to a recent version.

Bugs Fixed

- `decimal_round()` could cause a server exit when processing long numeric strings. (Bug #12563865)
- Passing a user variable as an argument to `GROUP_CONCAT()` could cause a server exit if the variable value changed during query execution. (Bug #12408412)
- `LOAD INDEX INTO CACHE` could cause a server exit if the index cache was too small. (Bug #12361113)
- A user with no privileges on a table could use a view to discover information about the table. (Bug #11765687)

Changes in MySQL 5.0.94 (2011-07-05)

End of Product Lifecycle. Active development for MySQL Database Server version 5.0 has ended. Oracle offers various support offerings which may be of interest. For details and more information, see the

MySQL section of the Lifetime Support Policy for Oracle Technology Products (<http://www.oracle.com/us/support/lifetime-support/index.html>). Please consider upgrading to a recent version.

Bugs Fixed

- Some files in the MySQL Server sources containing legacy code still used the LGPL license. Such files that were no longer in use have been removed. Any such code that remains following this removal now appears under the GPL only. (Bug #11896296)

References: See also: Bug #11840513.

- Under some circumstances, the result of `SUBSTRING_INDEX()` incorrectly depended on the contents of the previous row. (Bug #42404, Bug #11751514)

Changes in MySQL 5.0.93 (2011-05-05)

End of Product Lifecycle. Active development for MySQL Database Server version 5.0 has ended. Oracle offers various support offerings which may be of interest. For details and more information, see the MySQL section of the Lifetime Support Policy for Oracle Technology Products (<http://www.oracle.com/us/support/lifetime-support/index.html>). Please consider upgrading to a recent version.

Bugs Fixed

- **Security Fix:** The `PolyFromWKB()` function could crash the server when improper WKB data was passed to the function. (Bug #51875, Bug #11759554, CVE-2010-3840)
- **Security Fix:** A security bug was fixed. (Bug #49124)
- **Security Fix:** A security bug was fixed. (Bug #36544)
- Two unused test files in `storage/ndb/test/sql` contained incorrect versions of the GNU Lesser General Public License. The files and the directory containing them have been removed. (Bug #11810224)

References: See also: Bug #11810156.

- On FreeBSD and OpenBSD, the server incorrectly checked the range of the system date, causing legal values to be rejected. (Bug #55755, Bug #11763089)

Changes in MySQL 5.0.92 (2011-02-07)

End of Product Lifecycle. Active development for MySQL Database Server version 5.0 has ended. Oracle offers various support offerings which may be of interest. For details and more information, see the MySQL section of the Lifetime Support Policy for Oracle Technology Products (<http://www.oracle.com/us/support/lifetime-support/index.html>). Please consider upgrading to a recent version.

This section documents all changes and bugfixes that have been applied since the last MySQL Enterprise Server and MySQL Community Server release (5.0.91). If you would like to receive more fine-grained and personalized *update alerts* about fixes that are relevant to the version and features you use, please consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details please see <http://www.mysql.com/products/enterprise/advisors.html>.

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- The time zone tables available at <http://dev.mysql.com/downloads/timezones.html> have been updated. These tables can be used on systems such as Windows or HP-UX that do not include zoneinfo files. (Bug #40230)

Bugs Fixed

- **Security Fix:** A security bug was fixed. (Bug #57952)
- **Security Fix:** During evaluation of arguments to extreme-value functions such as `LEAST()` and `GREATEST()`, type errors did not propagate properly, causing the server to crash. (Bug #55826, CVE-2010-3833)
- **Security Fix:** The server could crash after materializing a derived table that required a temporary table for grouping. (Bug #55568, CVE-2010-3834)
- **Security Fix:** A user-variable assignment expression that is evaluated in a logical expression context can be precalculated in a temporary table for `GROUP BY`. However, when the expression value is used after creation of the temporary table, it was re-evaluated, not read from the table, and a server crash resulted. (Bug #55564, CVE-2010-3835)
- **Security Fix:** Joins involving a table with a unique `SET` column could cause a server crash. (Bug #54575, CVE-2010-3677)
- **Security Fix:** Pre-evaluation of `LIKE` predicates during view preparation could cause a server crash. (Bug #54568, Bug #11762026, CVE-2010-3836)
- **Security Fix:** `GROUP_CONCAT()` and `WITH ROLLUP` together could cause a server crash. (Bug #54476, CVE-2010-3837)
- **Security Fix:** Queries could cause a server crash if the `GREATEST()` or `LEAST()` function had a mixed list of numeric and `LONGBLOB` arguments, and the result of such a function was processed using an intermediate temporary table. (Bug #54461, CVE-2010-3838)
- **Security Fix:** A security bug was fixed. (Bug #53933)
- **Security Fix:** A security bug was fixed. (Bug #53907)
- **Security Fix:** Using `EXPLAIN` with queries of the form `SELECT ... UNION ... ORDER BY (SELECT ... WHERE ...)` could cause a server crash. (Bug #52711, CVE-2010-3682)
- **Security Fix:** A security bug was fixed. (Bug #52357)
- **Security Fix:** A security bug was fixed. (Bug #52315)
- **Security Fix:** A security bug was fixed. (Bug #48157)
- **InnoDB:** Creating or dropping a table with 1023 transactions active caused an assertion failure. (Bug #49238)
- The `make_binary_distribution` target to `make` could fail on some platforms because the lines generated were too long for the shell. (Bug #54590)
- A client could supply data in chunks to a prepared statement parameter other than of type `TEXT` or `BLOB` using the `mysql_stmt_send_long_data()` C API function (or `COM_STMT_SEND_LONG_DATA` command). This led to a crash because other data types are not valid for long data. (Bug #54041)
- Builds of the embedded `mysqld` failed due to a missing element of the `struct NET`. (Bug #53908, Bug #53912)

- The definition of the `MY_INIT` macro in `my_sys.h` included an extraneous semicolon, which could cause compilation failure. (Bug #53906)
- If the remote server for a `FEDERATED` table could not be accessed, queries for the `INFORMATION_SCHEMA.TABLES` table failed. (Bug #35333)
- `mysqld` could fail during execution when using SSL. (Bug #34236)
- Threads that were calculating the estimated number of records for a range scan did not respond to the `KILL` statement. That is, if a `range` join type is possible (even if not selected by the optimizer as a join type of choice and thus not shown by `EXPLAIN`), the query in the `statistics` state (shown by the `SHOW PROCESSLIST`) did not respond to the `KILL` statement. (Bug #25421)

Changes in MySQL 5.0.91 (2010-05-05)

End of Product Lifecycle. Active development for MySQL Database Server version 5.0 has ended. Oracle offers various support offerings which may be of interest. For details and more information, see the MySQL section of the Lifetime Support Policy for Oracle Technology Products (<http://www.oracle.com/us/support/lifetime-support/index.html>). Please consider upgrading to a recent version.

This section documents all changes and bugfixes that have been applied since the last MySQL Enterprise Server and MySQL Community Server release (5.0.90). If you would like to receive more fine-grained and personalized *update alerts* about fixes that are relevant to the version and features you use, please consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details please see <http://www.mysql.com/products/enterprise/advisors.html>.

- [icc Notes](#)
- [Bugs Fixed](#)

icc Notes

- This is the final release of MySQL 5.0 for which Generic Linux MySQL binary packages built with the `icc` compiler on x86 and x86_64 will be offered. These were previously produced as an alternative to our main packages built using `gcc`, as they provided noticeable performance benefits. In recent times the performance differences have diminished and build and runtime problems have surfaced, thus it is no longer viable to continue producing them.

We continue to use the `icc` compiler to produce our distribution-specific RPM packages on ia64.

Bugs Fixed

- **Security Fix:** The server failed to check the table name argument of a `COM_FIELD_LIST` command packet for validity and compliance to acceptable table name standards. This could be exploited to bypass almost all forms of checks for privileges and table-level grants by providing a specially crafted table name argument to `COM_FIELD_LIST`.

In MySQL 5.0 and above, this permitted an authenticated user with `SELECT` privileges on one table to obtain the field definitions of any table in all other databases and potentially of other MySQL instances accessible from the server's file system.

Additionally, for MySQL version 5.1 and above, an authenticated user with `DELETE` or `SELECT` privileges on one table could delete or read content from any other table in all databases on this server, and potentially of other MySQL instances accessible from the server's file system. (Bug #53371, CVE-2010-1848)

- **Security Fix:** The server was susceptible to a buffer-overflow attack due to a failure to perform bounds checking on the table name argument of a `COM_FIELD_LIST` command packet. By sending long data

for the table name, a buffer is overflowed, which could be exploited by an authenticated user to inject malicious code. (Bug #53237, CVE-2010-1850)

- **Security Fix:** The server could be tricked into reading packets indefinitely if it received a packet larger than the maximum size of one packet. (Bug #50974, CVE-2010-1849)
- The optimizer could attempt to evaluate the `WHERE` clause before any rows had been read, resulting in a server crash. (Bug #52177)
- On Windows, `LOAD_FILE()` could cause a crash for some pathnames. (Bug #51893)
- Use of `HANDLER` statements with tables that had spatial indexes caused a server crash. (Bug #51357)
- With an XA transaction active, `SET autocommit = 1` could cause side effects such as memory corruption or a server crash. (Bug #51342)
- The SSL certificates in the test suite were about to expire. They have been updated with expiration dates in the year 2015. (Bug #50642)
- For debug builds, an assertion was incorrectly raised in the optimizer when matching `ORDER BY` expressions. (Bug #50335)
- The `filesort` sorting method applied to a `CHAR(0)` column could lead to a server crash. (Bug #49897)
- `sql_buffer_result` had an effect on non-`SELECT` statements, contrary to the documentation. (Bug #49552)
- `EXPLAIN EXTENDED` crashed trying to print column names for a subquery in the `FROM` clause when the table had gone out of scope. (Bug #49487)
- `mysql-test-run.pl` now recognizes the `MTR_TESTCASE_TIMEOUT`, `MTR_SUITE_TIMEOUT`, `MTR_SHUTDOWN_TIMEOUT`, and `MTR_START_TIMEOUT` environment variables. If they are set, their values are used to set the `--testcase-timeout`, `--suite-timeout`, `--shutdown-timeout`, and `--start-timeout` options, respectively. (Bug #49210)
- Certain `INTERVAL` expressions could cause a crash on 64-bit systems. (Bug #48739)
- The server crashed when it could not determine the best execution plan for queries involving outer joins with nondeterministic `ON` clauses such as the ones containing the `RAND()` function, a user-defined function, or a `NOT DETERMINISTIC` stored function. (Bug #48483)
- If an outer query was invalid, a subquery might not be set up. `EXPLAIN EXTENDED` did not expect this and caused a crash by trying to dereference improperly set up information. (Bug #48295)

Changes in MySQL 5.0.90 (2010-01-15)

End of Product Lifecycle. Active development for MySQL Database Server version 5.0 has ended. Oracle offers various support offerings which may be of interest. For details and more information, see the MySQL section of the Lifetime Support Policy for Oracle Technology Products (<http://www.oracle.com/us/support/lifetime-support/index.html>). Please consider upgrading to a recent version.

This section documents all changes and bugfixes that have been applied since the last MySQL Enterprise Server and MySQL Community Server release (5.0.89). If you would like to receive more fine-grained and personalized *update alerts* about fixes that are relevant to the version and features you use, please consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details please see <http://www.mysql.com/products/enterprise/advisors.html>.

Bugs Fixed

- **Security Fix:** For servers built with yaSSL, a preauthorization buffer overflow could cause memory corruption or a server crash. We thank Evgeny Legerov from Intevydis for providing us with a proof-of-concept script that permitted us to reproduce this bug. (Bug #50227, CVE-2009-4484)
- **Replication:** `FLUSH LOGS` did not close and reopen the binary log index file. (Bug #48738)
References: See also: Bug #34582.
- Some prepared statements could raise an assertion when re-executed. (Bug #49570)
- Valgrind warnings for `CHECKSUM TABLE` were corrected. (Bug #49465)
- Specifying an index algorithm (such as `BTREE`) for `SPATIAL` or `FULLTEXT` indexes caused a server crash. These index types do not support algorithm specification, and it is not longer permitted to do so. (Bug #49250)
- The optimizer sometimes incorrectly handled conditions of the form `WHERE col_name='const1' AND col_name='const2'`. (Bug #49199)
- Several `strmake()` calls had an incorrect length argument (too large by one). (Bug #48983)
- On Fedora 12, `strmov()` did not guarantee correct operation for overlapping source and destination buffer. Calls were fixed to use an overlap-safe version instead. (Bug #48866)
- Incomplete reset of internal `TABLE` structures could cause a crash with `eq_ref` table access in subqueries. (Bug #48709)
- Re-execution of a prepared statement could cause a server crash. (Bug #48508)
- The error message for `ER_UPDATE_INFO` was subject to buffer overflow or truncation. (Bug #48500)
- On Solaris, the server printed no stack trace to the error log after a crash. (Bug #47391)
- A crash occurred when a user variable that was assigned to a subquery result was used as a result field in a `SELECT` statement with aggregate functions. (Bug #47371)
- Comparison with `NULL` values sometimes did not produce a correct result. (Bug #42760)
- When compressed `MyISAM` files were opened, they were always memory mapped, sometimes causing memory-swapping problems. To deal with this, a new system variable, `myisam_mmap_size`, was added to permit limiting the amount of memory used for memory mapping of `MyISAM` files. (Bug #37408)

Changes in MySQL 5.0.89 (2009-12-02)

End of Product Lifecycle. Active development for MySQL Database Server version 5.0 has ended. Oracle offers various support offerings which may be of interest. For details and more information, see the MySQL section of the Lifetime Support Policy for Oracle Technology Products (<http://www.oracle.com/us/support/lifetime-support/index.html>). Please consider upgrading to a recent version.

This section documents all changes and bugfixes that have been applied since the last MySQL Enterprise Server and MySQL Community Server release (5.0.88). If you would like to receive more fine-grained and personalized *update alerts* about fixes that are relevant to the version and features you use, please consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details please see <http://www.mysql.com/products/enterprise/advisors.html>.

Bugs Fixed

- Privileges for stored routines were ignored for mixed-case routine names. (Bug #48872)

References: See also: Bug #41049.

- Building MySQL on Fedora Core 12 64-bit failed, due to errors in `comp_err`. (Bug #48864)
- `DISTINCT` was ignored for queries with `GROUP BY WITH ROLLUP` and only `const` tables. (Bug #48475)
- Loose index scan was inappropriately chosen for some `WHERE` conditions. (Bug #48472)
- A bad typecast could cause query execution to allocate large amounts of memory. (Bug #48458)
- `mysql_secure_installation` did not work on Solaris. (Bug #48086)
- When running `mysql_secure_installation`, the command failed if the `root` password contained multiple space, `'\'`, `'#'`, or quote characters. (Bug #48031)
- `InnoDB` did not disallow creation of an index with the name `GEN_CLUST_INDEX`, which is used internally. (Bug #46000)
- Use of `InnoDB` monitoring (`SHOW ENGINE INNODB STATUS` or one of the `InnoDB` Monitor tables) could cause a server crash due to invalid access to a shared variable in a concurrent environment. (Bug #38883)
- Output from `mysql --html` did not encode the `'<'`, `'>'`, or `'&'` characters. (Bug #27884)

Changes in MySQL 5.0.88 (2009-11-04)

This section documents all changes and bugfixes that have been applied since the last MySQL Enterprise Server and MySQL Community Server release (5.0.87). If you would like to receive more fine-grained and personalized *update alerts* about fixes that are relevant to the version and features you use, please consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details please see <http://www.mysql.com/products/enterprise/advisors.html>.

Bugs Fixed

- **Security Fix:** MySQL clients linked against OpenSSL could be tricked not to check server certificates. (Bug #47320, CVE-2009-4028)
- **MySQL Cluster:** When a data node had written its GCI marker to the first page of a megabyte, and that node was later killed during restart after having processed that page (marker) but before completing a LCP, the data node could fail with file system errors. (Bug #44952)

References: See also: Bug #42564, Bug #44291.

- **Replication:** When a session was closed on the master, temporary tables belonging to that session were logged with the wrong database names when either of the following conditions was true:
 1. The length of the name of the database to which the temporary table belonged was greater than the length of the current database name.
 2. The current database was not set.

(Bug #48216)

References: See also: Bug #46861, Bug #48297.

- A query containing a view using temporary tables and multiple tables in the `FROM` clause and `PROCEDURE ANALYSE()` caused a server crash.

As a result of this bug fix, `PROCEDURE ANALYSE()` is legal only in a top-level `SELECT`. (Bug #48293)

References: See also: Bug #46184.

- Error handling was missing for `SELECT` statements containing subqueries in the `WHERE` clause and that assigned a `SELECT` result to a user variable. The server could crash as a result. (Bug #48291)
- An assertion could fail if the optimizer used a `SPATIAL` index. (Bug #48258, Bug #47019)
- A combination of `GROUP BY WITH ROLLUP`, `DISTINCT` and the `const` join type in a query caused a server crash when the optimizer used a temporary table to resolve `DISTINCT`. (Bug #48131)
- `mysys/mf_keycache.c` requires threading, but no test was made for thread support. (Bug #47923)
- If the first argument to `GeomFromWKB()` function was a geometry value, the function just returned its value. However, it failed to preserve the argument's `null_value` flag, which caused an unexpected `NULL` value to be returned to the caller, resulting in a server crash. (Bug #47780)
- The GPL and commercial license headers had different sizes, so that error log, backtrace, core dump, and cluster trace file line numbers could be off by one if they were not checked against the version of the source used for the build. (For example, checking a GPL build backtrace against commercial sources.) (Bug #46216)
- During the build of the Red Hat IA64 MySQL server RPM, the system library link order was incorrect. This made the resulting Red Hat IA64 RPM depend on "libc.so.6.1(GLIBC_PRIVATE)(64bit)", thus preventing installation of the package. (Bug #45706)
- Failure to treat `BIT` values as unsigned could lead to unpredictable results. (Bug #42803)
- Some queries with nested outer joins could lead to crashes or incorrect results because an internal data structure was handled improperly. (Bug #42116)
- In a replication scenario with `innodb_locks_unsafe_for_binlog` enabled on the slave, where rows were changed only on the slave (not through replication), in some rare cases, many messages of the following form were written to the slave error log: `InnoDB: Error: unlock row could not find a 4 mode lock on the record.` (Bug #41756)
- A stub of the previously removed `mysql_odbc_escape_string()` function was restored to fix a ABI breakage. The function was intended to be private and used only by Connector/ODBC, but, unfortunately, it was exported as part of the ABI. Nonetheless, only a stub is restored as the original function is inherently broken and should not be used. (Bug #41728)

References: See also: Bug #29592.

- After renaming a user, granting that user privileges could result in the user having privileges additional to those granted. (Bug #41597)
- In some cases, the server did not recognize lettercase differences between `GRANT` attributes such as table name or user name. For example, a user was able to perform operations on a table with privileges of another user with the same user name but in a different lettercase.

In consequence of this bug fix, the collation for the `Routine_name` column of the `mysql.proc` table is changed from `utf8_bin` to `utf8_general_ci`. (Bug #41049)

References: See also: Bug #48872.

Changes in MySQL Enterprise 5.0.87sp1 [QSP] (2010-02-03)

This is a *Service Pack* release of the MySQL Enterprise Server 5.0.

This section documents all changes and bugfixes that have been applied since the last MySQL Enterprise Server release (5.0.87).

If you would like to receive more fine-grained and personalized *update alerts* about fixes that are relevant to the version and features you use, please consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details please see <http://www.mysql.com/products/enterprise/advisors.html>.

Bugs Fixed

- **Security Fix:** For servers built with yaSSL, a preauthorization buffer overflow could cause memory corruption or a server crash. We thank Evgeny Legerov from Intevydis for providing us with a proof-of-concept script that permitted us to reproduce this bug. (Bug #50227, CVE-2009-4484)
- **Replication:** When a session was closed on the master, temporary tables belonging to that session were logged with the wrong database names when either of the following conditions was true:
 1. The length of the name of the database to which the temporary table belonged was greater than the length of the current database name.
 2. The current database was not set.

(Bug #48216)

References: See also: Bug #46861, Bug #48297.

- Specifying an index algorithm (such as `BTREE`) for `SPATIAL` or `FULLTEXT` indexes caused a server crash. These index types do not support algorithm specification, and it is not longer permitted to do so. (Bug #49250)
- Building MySQL on Fedora Core 12 64-bit failed, due to errors in `comp_err`. (Bug #48864)
- Re-execution of a prepared statement could cause a server crash. (Bug #48508)
- A bad typecast could cause query execution to allocate large amounts of memory. (Bug #48458)
- A query containing a view using temporary tables and multiple tables in the `FROM` clause and `PROCEDURE ANALYSE()` caused a server crash.

As a result of this bug fix, `PROCEDURE ANALYSE()` is legal only in a top-level `SELECT`. (Bug #48293)

References: See also: Bug #46184.

- Error handling was missing for `SELECT` statements containing subqueries in the `WHERE` clause and that assigned a `SELECT` result to a user variable. The server could crash as a result. (Bug #48291)
- An assertion could fail if the optimizer used a `SPATIAL` index. (Bug #48258, Bug #47019)
- A combination of `GROUP BY WITH ROLLUP`, `DISTINCT` and the `const` join type in a query caused a server crash when the optimizer used a temporary table to resolve `DISTINCT`. (Bug #48131)
- If the first argument to `GeomFromWKB()` function was a geometry value, the function just returned its value. However, it failed to preserve the argument's `null_value` flag, which caused an unexpected `NULL` value to be returned to the caller, resulting in a server crash. (Bug #47780)
- In a replication scenario with `innodb_locks_unsafe_for_binlog` enabled on the slave, where rows were changed only on the slave (not through replication), in some rare cases, many messages of the following form were written to the slave error log: `InnoDB: Error: unlock row could not find a 4 mode lock on the record`. (Bug #41756)

- In some cases, the server did not recognize lettercase differences between `GRANT` attributes such as table name or user name. For example, a user was able to perform operations on a table with privileges of another user with the same user name but in a different lettercase.

In consequence of this bug fix, the collation for the `Routine_name` column of the `mysql.proc` table is changed from `utf8_bin` to `utf8_general_ci`. (Bug #41049)

References: See also: Bug #48872.

- Use of `InnoDB` monitoring (`SHOW ENGINE INNODB STATUS` or one of the `InnoDB` Monitor tables) could cause a server crash due to invalid access to a shared variable in a concurrent environment. (Bug #38883)

Changes in MySQL 5.0.87 (2009-10-15)

This section documents all changes and bugfixes that have been applied since the last MySQL Enterprise Server and MySQL Community Server release (5.0.86). If you would like to receive more fine-grained and personalized *update alerts* about fixes that are relevant to the version and features you use, please consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details please see <http://www.mysql.com/products/enterprise/advisors.html>.

Bugs Fixed

- **Incompatible Change:** In binary installations of MySQL, the supplied `binary-configure` script would start and configure MySQL, even when command help was requested with the `--help` command-line option. The `--help` option, if provided, no longer starts and installs the server. (Bug #30954)
- **Replication:** `BEGIN` statements were not included in the output of `mysqlbinlog`. (Bug #46998)
- **Replication:** Database-level character sets were not always honored by the replication SQL thread. This could cause data inserted on the master using `LOAD DATA` to be replicated using the wrong character set. (Bug #45516)
- **API:** The fix for Bug #24507 could lead in some cases to client application failures due to a race condition. Now the server waits for the “dummy” thread to return before exiting, thus making sure that only one thread can initialize the POSIX threads library. (Bug #42850)

References: This issue is a regression of: Bug #24507.

- On Mac OS X or Windows, sending a `SIGHUP` signal to the server or an asynchronous flush (triggered by `flush_time`) caused the server to crash. (Bug #47525)
- Solaris binary packages now are compiled with `-g0` rather than `-g`. (Bug #47137)
- `EXPLAIN` caused a server crash for certain valid queries. (Bug #47106)
- When creating a new instance on Windows using `mysqld-nt` and the `--install` parameter, the value of the service would be set incorrectly, resulting in a failure to start the configured service. (Bug #46917)
- `CONCAT_WS()` could return incorrect results due to an argument buffer also being used as a result buffer. (Bug #46815)
- The server crashed when re-using outer column references in correlated subqueries when the enclosing query used a temp table. (Bug #46791)
- The server ignored the setting of `sync_frm` for `CREATE TABLE ... LIKE`. (Bug #46591)

- An attempt to create a table with the same name as an existing view could cause a server crash. (Bug #46384)
- A memory leak occurred when `EXPLAIN` encountered a malformed query. (Bug #45989)
- When re-installing MySQL on Windows on a server that has a data directory from a previous MySQL installation, the installer failed to identify the existence of the installation and the password configured for the `root` user. (Bug #45200)
- Client flags were incorrectly initialized for the embedded server, causing several tests in the `jp` test suite to fail. (Bug #45159)
- A test for stack growth failed on some platforms, leading to server crashes. (Bug #42213)

References: See also: Bug #62856.

- The server used the wrong lock type (always `TL_READ` instead of `TL_READ_NO_INSERT` when appropriate) for tables used in subqueries of `UPDATE` statements. This led in some cases to replication failure because statements were written in the wrong order to the binary log. (Bug #42108)
- Concurrent execution of `FLUSH TABLES` along with `SHOW FUNCTION STATUS` or `SHOW PROCEDURE STATUS` could cause a server crash. (Bug #34895)
- `myisamchk` performed parameter value casting at startup that generated unnecessary warning messages. (Bug #33785)
- When building MySQL on Windows from source, the `WITH_BERKELEY_STORAGE_ENGINE` option would fail to configure `BDB` support correctly. (Bug #27693)
- Changing the size of a key buffer that is under heavy use could cause a server crash. The fix partially removes the limitation that `LOAD INDEX INTO CACHE` fails unless all indexes in a table have the same block size. Now the statement fails only if `IGNORE LEAVES` is specified. (Bug #17332)

Changes in MySQL 5.0.86 (2009-09-09)

This section documents all changes and bugfixes that have been applied since the last MySQL Enterprise Server and MySQL Community Server release (5.0.85). If you would like to receive more fine-grained and personalized *update alerts* about fixes that are relevant to the version and features you use, please consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details please see <http://www.mysql.com/products/enterprise/advisors.html>.

Bugs Fixed

- **Performance:** For `MyISAM` tables with `bulk_insert_buffer_size` values larger than 256KB, the performance of bulk insert operations such as multiple-row `INSERT` and `INSERT ... SELECT` operations has been improved greatly when up to a hundred rows are inserted at the same time. (Bug #44723)
- **Replication:** When using the `--replicate-rewrite-db` option and the database referenced by this option on the master was the current database when the connection to the slave was closed, any temporary tables existing in this database were not properly dropped. (Bug #46861)
- **Replication:** In some cases, a `STOP SLAVE` statement could cause the replication slave to crash. This issue was specific to MySQL on Windows or Macintosh platforms. (Bug #45238, Bug #45242, Bug #45243, Bug #46013, Bug #46014, Bug #46030)

References: See also: Bug #40796.

- Stack overflow checking did not account for the size of the structure stored in the heap. (Bug #46807)
- The server could crash for queries with the following elements: 1. An “impossible where” in the outermost `SELECT`; 2. An aggregate in the outermost `SELECT`; 3. A correlated subquery with a `WHERE` clause that includes an outer field reference as a top-level `WHERE` sargable predicate; (Bug #46749)
- `CREATE TABLE ... SELECT` could cause assertion failure if a table already existed with the same name and contained an `AUTO_INCREMENT` column. (Bug #46616)
- A query containing a subquery in the `FROM` clause and `PROCEDURE ANALYSE()` caused a server crash. (Bug #46184)

References: See also: Bug #48293.

- If `--basedir` was specified, `mysqld_safe` did not use it when attempting to locate `my_print_defaults`. (Bug #39326)
- A buffer overflow could occur during handling of `IS NULL` ranges. (Bug #37044)
- `mysqladmin --wait ping` crashed on Windows systems. (Bug #35132)

Changes in MySQL 5.0.85 (2009-08-11)

This section documents all changes and bugfixes that have been applied since the last MySQL Enterprise Server and MySQL Community Server release (5.0.84). If you would like to receive more fine-grained and personalized *update alerts* about fixes that are relevant to the version and features you use, please consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details please see <http://www.mysql.com/products/enterprise/advisors.html>.

Bugs Fixed

- **Important Change:** Uninstalling MySQL using the MySQL installer on Windows would delete the `my.ini` file. The file is no longer deleted. In addition, when a new installation is conducted, any existing configuration file will be renamed to `myDATETIME.ini.bak` during configuration. (Bug #36493)
- The server printed warnings at startup about adjusting the value of the `max_join_size` system variable. (These were harmless, but might be seen by users as significant.) (Bug #46385)
- The server crashed if evaluation of `GROUP_CONCAT(... ORDER BY)` required allocation of a sort buffer but allocation failed. (Bug #46080)
- After an error such as a table-full condition, `INSERT IGNORE` could cause an assertion failure for debug builds. (Bug #46075)
- An optimization that moved an item from a subquery to an outer query could cause a server crash. (Bug #46051)
- Several Valgrind warnings were corrected. (Bug #46003, Bug #46034, Bug #46042)
- For problems reading SSL files during SSL initialization, the server wrote error messages to `stderr` rather than to the error log. (Bug #45770)
- The vendor name change from MySQL AB to Sun Microsystems, Inc. in RPM packages was not handled gracefully when upgrading MySQL using an RPM package. (Bug #45534)
- A Windows Installation using the GUI installer failed with:

```
MySQL Server 5.1 Setup Wizard ended prematurely
```

```
The wizard was interrupted before MySQL Server 5.1. could be completely installed.
```

```
Your system has not been modified. To complete installation at another time, please run setup again.
```

```
Click Finish to exit the wizard
```

This was due to a step in the MSI installer that could fail to execute correctly on some environments. (Bug #45418)

- Compiler warnings on Windows were fixed. (Bug #45287)
- Invalid memory reads could occur using the compressed client/server protocol. (Bug #45031)
- Invalid input could cause invalid memory reads by the parser. (Bug #45010)
- Creating a new instance after previously removing an instance failed to complete the installation properly because the security settings could not be applied correctly. (Bug #44428)
- The server did not always check the return value of calls to the `hash_init()` function. (Bug #43572)
- A test for stack growth failed on some platforms, leading to server crashes. (Bug #42213)

References: See also: Bug #62856.

- `SHOW PROCESSLIST` could access freed memory of a stored procedure run in a concurrent session. (Bug #38816)
- During installation on Windows, the MySQL Instance Configuration Wizard window could be opened at a size too small to be usable. (Bug #38723)
- `make_binary_distribution` did not always generate correct distribution names. (Bug #37808)
- The server crashed when executing a prepared statement containing a duplicated `MATCH()` function call in the select list and `ORDER BY` clause; for example, `SELECT MATCH(a) AGAINST('test') FROM t1 ORDER BY MATCH(a) AGAINST('test')`. (Bug #37740)
- When performing an installation on Windows using the GUI installer, the installer failed to wait long enough during installation for the MySQL service to be installed, which would cause the installation to fail and may cause security settings, such as the `root` password to not be applied correctly. (Bug #30525)
- If `InnoDB` reached its limit on the number of concurrent transactions (1023), it wrote a descriptive message to the error log but returned a misleading error message to the client, or an assertion failure occurred. (Bug #18828)

References: See also: Bug #46672.

- Installation of MySQL on Windows failed to set the correct location for the character set files, which could lead to `mysqld` and `mysql` failing to initialize properly. (Bug #17270)

Changes in MySQL Enterprise 5.0.84sp1 [QSP] (2009-09-30)

This is a *Service Pack* release of the MySQL Enterprise Server 5.0.

This section documents all changes and bugfixes that have been applied since the last MySQL Enterprise Server release (5.0.84).

If you would like to receive more fine-grained and personalized *update alerts* about fixes that are relevant to the version and features you use, please consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details please see <http://www.mysql.com/products/enterprise/advisors.html>.

Bugs Fixed

- **Important Change:** Uninstalling MySQL using the MySQL installer on Windows would delete the `my.ini` file. The file is no longer deleted. In addition, when a new installation is conducted, any existing configuration file will be renamed to `myDATETIME.ini.bak` during configuration. (Bug #36493)
- The server could crash for queries with the following elements: 1. An “impossible where” in the outermost `SELECT`; 2. An aggregate in the outermost `SELECT`; 3. A correlated subquery with a `WHERE` clause that includes an outer field reference as a top-level `WHERE` sargable predicate; (Bug #46749)
- A query containing a subquery in the `FROM` clause and `PROCEDURE ANALYSE()` caused a server crash. (Bug #46184)

References: See also: Bug #48293.

- A Windows Installation using the GUI installer failed with:

```
MySQL Server 5.1 Setup Wizard ended prematurely

The wizard was interrupted before MySQL Server 5.1. could be completely installed.

Your system has not been modified. To complete installation at another time, please run
setup again.

Click Finish to exit the wizard
```

This was due to a step in the MSI installer that could fail to execute correctly on some environments. (Bug #45418)

Changes in MySQL 5.0.84 (2009-07-07)

This section documents all changes and bugfixes that have been applied since the last MySQL Enterprise Server and MySQL Community Server release (5.0.83). If you would like to receive more fine-grained and personalized *update alerts* about fixes that are relevant to the version and features you use, please consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details please see <http://www.mysql.com/products/enterprise/advisors.html>.

Bugs Fixed

- **Security Fix:** A suitable database identifier supplied to the `COM_CREATE_DB` or `COM_DROP_DB` command could cause a segmentation fault, and thereby a denial of service. (Bug #45790, CVE-2009-2446)
- **Security Fix:** The server crashed if an account with the `CREATE ROUTINE` privilege but not the `EXECUTE` privilege attempted to create a stored procedure. (Bug #44798)
- **Performance:** The `InnoDB` adaptive hash latch is released (if held) for several potentially long-running operations. This improves throughput for other queries if the current query is removing a temporary table, changing a temporary table from memory to disk, using `CREATE TABLE ... SELECT`, or performing a `MyISAM` repair on a table used within a transaction. (Bug #32149)
- **Important Change; Replication:** `BEGIN`, `COMMIT`, and `ROLLBACK` statements are no longer affected by `--replicate-do-db` or `--replicate-ignore-db` rules. (Bug #43263)
- **Replication:** When reading a binary log that was in use by a master or that had not been properly closed (possibly due to a crash), the following message was printed: `Warning: this binlog was not closed properly. Most probably mysqld crashed writing it.` This message did not take into account the possibility that the file was merely in use by the master, which caused some users concern who were not aware that this could happen.

To make this clear, the original message has been replaced with `Warning: this binlog is either is use or was not closed properly.` (Bug #34687)

- The server crashed for attempts to use `REPLACE` or `INSERT ... ON DUPLICATE KEY UPDATE` with a view defined using a join. (Bug #45806)
- The combination of `MIN()` or `MAX()` in the select list with `WHERE` and `GROUP BY` clauses could lead to incorrect results. (Bug #45386)
- Compiler warnings on Mac OS X were fixed. (Bug #45286)
- The `mysql` client could misinterpret some character sequences as commands under some circumstances. (Bug #45236)
- Use of `ROUND()` on a `LONGTEXT` or `LONGBLOB` column of a derived table could cause a server crash. (Bug #45152)
- Index Merge followed by a filesort could result in a server crash if `sort_buffer_size` was not large enough for all sort keys. (Bug #44810)

References: See also: Bug #40974.

- The `PASSWORD()` and `OLD_PASSWORD()` functions could read memory outside of an internal buffer when used with `BLOB` arguments. (Bug #44767)
- Some Perl scripts in AIX packages contained an incorrect path to the `perl` executable. (Bug #44643)
- A workaround for a Sun Studio bug was instituted. (Bug #41710)
- Shared-memory connections did not work in Vista if `mysqld` was started from the command line. (Bug #41190)
- Some `UPDATE` statements that affected no rows returned a rows-affected count of one. (Bug #40565)
- Valgrind warnings that occurred for `SHOW TABLE STATUS` with `InnoDB` tables were silenced. (Bug #38479)
- In the `mysql` client, using a default character set of `binary` caused internal commands such as `DELIMITER` to become case sensitive. (Bug #37268)
- A Valgrind error during subquery execution was corrected. (Bug #36995)
- When invoked to start multiple server instances, `mysqld_multi` sometimes failed to start them all due to not changing location into the base directory for each instance. (Bug #36654)
- On Windows, the `_PC` macro in `my_global.h` was causing problems for modern compilers. It has been removed because it is no longer used. (Bug #34309)
- Setting the session value of the `max_allowed_packet` or `net_buffer_length` system variable was permitted but had no effect. The session value of these variables is now read only. (Bug #32223)

References: See also: Bug #22891.

Changes in MySQL 5.0.83 (2009-05-29)

This section documents all changes and bugfixes that have been applied since the last MySQL Enterprise Server and MySQL Community Server release (5.0.82). If you would like to receive more fine-grained and personalized *update alerts* about fixes that are relevant to the version and features you use, please

consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details please see <http://www.mysql.com/products/enterprise/advisors.html>.

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- The time zone tables available at <http://dev.mysql.com/downloads/timezones.html> have been updated. These tables can be used on systems such as Windows or HP-UX that do not include zoneinfo files. (Bug #39923)

Bugs Fixed

- **Replication:** When stopping and restarting the slave while it was replicating temporary tables, the slave server could crash or raise an assertion failure. This was due to the fact that, although temporary tables were saved between slave thread restarts, the reference to the thread being used (`table->in_use`) was not being properly updated when restarting, continuing to reference the old thread instead of the new one. This issue affected statement-based replication only. (Bug #41725)
- `UNCOMPRESSED_LENGTH()` returned a garbage result when passed a string shorter than 5 bytes. Now `UNCOMPRESSED_LENGTH()` returns `NULL` and generates a warning. (Bug #44796)
- Several Valgrind warnings were silenced. (Bug #44774, Bug #44792)
- Incorrect time was reported at the end of `mysqldump` output. (Bug #44424)
- `EXPLAIN EXTENDED` could crash for `UNION` queries in which the last `SELECT` was not parenthesized and included an `ORDER BY` clause. (Bug #43612)
- `SELECT ... INTO @var` could produce values different from `SELECT ...` without the `INTO` clause. (Bug #42009)
- Using `--hexdump` together with `--read-from-remote-server` caused `mysqlbinlog` to crash. (Bug #41943)
- A crash occurred due to a race condition between the merge table and `table_cache` evictions.

```
00000001403C452F  mysql_d.exe!memcpy()[memcpy.asm:151]
00000001402A275F  mysql_d.exe!ha_myisammrg::info()[ha_myisammrg.cc:854]
00000001402A2471  mysql_d.exe!ha_myisammrg::attach_children()[ha_myisammrg.cc:488]
00000001402A2788  mysql_d.exe!ha_myisammrg::extra()[ha_myisammrg.cc:863]
000000014015FC5D  mysql_d.exe!attach_merge_children()[sql_base.cc:4135]
000000014016A4C1  mysql_d.exe!open_tables()[sql_base.cc:4697]
000000014016A898  mysql_d.exe!open_and_lock_tables_derived()[sql_base.cc:4956]
000000014018BB54  mysql_d.exe!mysql_insert()[sql_insert.cc:613]
000000014019EDD3  mysql_d.exe!mysql_execute_command()[sql_parse.cc:3066]
00000001401A2F06  mysql_d.exe!mysql_parse()[sql_parse.cc:5791]
00000001401A3C1A  mysql_d.exe!dispatch_command()[sql_parse.cc:1202]
00000001401A4CD7  mysql_d.exe!do_command()[sql_parse.cc:857]
0000000140246327  mysql_d.exe!handle_one_connection()[sql_connect.cc:1115]
00000001402B82C5  mysql_d.exe!pthread_start()[my_winthread.c:85]
00000001403CAC37  mysql_d.exe!_callthreadstart()[thread.c:295]
00000001403CAD05  mysql_d.exe!_threadstart()[thread.c:275]
000000077D6B69A  kernel32.dll!BaseThreadStart()
Trying to get some variables.
Some pointers may be invalid and cause the dump to abort...
```

(Bug #41212)

- For some queries, an equality propagation problem could cause `a = b` and `b = a` to be handled differently. (Bug #40925)
- For views created with a column list clause, column aliases were not substituted when selecting through the view using a `HAVING` clause. (Bug #40825)
- A multiple-table `DELETE` involving a table self-join could cause a server crash. (Bug #39918)
- Creating an `InnoDB` table with a comment containing a '#' character caused foreign key constraints to be omitted. (Bug #39793)
- The `mysql` option `--ignore-spaces` was nonfunctional. (Bug #39101)
- If a query was such as to produce the error `1054 Unknown column '...' in 'field list'`, using `EXPLAIN EXTENDED` with the query could cause a server crash. (Bug #37362)

Changes in MySQL Enterprise 5.0.82sp1 [QSP] (2009-07-21)

This is a *Service Pack* release of the MySQL Enterprise Server 5.0.

This section documents all changes and bugfixes that have been applied since the last MySQL Enterprise Server release (5.0.82).

If you would like to receive more fine-grained and personalized *update alerts* about fixes that are relevant to the version and features you use, please consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details please see <http://www.mysql.com/products/enterprise/advisors.html>.

Bugs Fixed

- The server crashed for attempts to use `REPLACE` or `INSERT ... ON DUPLICATE KEY UPDATE` with a view defined using a join. (Bug #45806)
- Use of `ROUND()` on a `LONGTEXT` or `LONGBLOB` column of a derived table could cause a server crash. (Bug #45152)
- Index Merge followed by a filesort could result in a server crash if `sort_buffer_size` was not large enough for all sort keys. (Bug #44810)

References: See also: Bug #40974.

- If a query was such as to produce the error `1054 Unknown column '...' in 'field list'`, using `EXPLAIN EXTENDED` with the query could cause a server crash. (Bug #37362)

Changes in MySQL 5.0.82 (2009-05-20)

This section documents all changes and bugfixes that have been applied since the last MySQL Enterprise Server and MySQL Community Server release (5.0.80). If you would like to receive more fine-grained and personalized *update alerts* about fixes that are relevant to the version and features you use, please consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details please see <http://www.mysql.com/products/enterprise/advisors.html>.

Bugs Fixed

- **Performance:** `InnoDB` uses random numbers to generate dives into indexes for calculating index cardinality. However, under certain conditions, the algorithm did not generate random numbers, so `ANALYZE TABLE` did not update cardinality estimates properly. A new algorithm has been introduced with better randomization properties, together with a system variable, `innodb_use_legacy_cardinality_algorithm`, that controls which algorithm to use. The default

value of the variable is 1 (**ON**), to use the original algorithm for compatibility with existing applications. The variable can be set to 0 (**OFF**) to use the new algorithm with improved randomness. (Bug #43660)

- **Replication:** Restarting the replication slave—either by using **STOP SLAVE** plus **START SLAVE**, or by restarting the slave `mysqld` process—could sometimes cause the slave to crash when using a debug version of the server. (Bug #38694)
- **Replication:** Killing the thread executing a DDL statement, after it had finished its execution but before it had written the binary log event, caused the error code in the binary log event to be set (incorrectly) to **ER_SERVER_SHUTDOWN** or **ER_QUERY_INTERRUPTED**, which caused replication to fail. (Bug #37145)

References: See also: Bug #27571, Bug #22725.

- **Replication:** Column aliases used inside subqueries were ignored in the binary log. (Bug #35515)
- **Replication:** The statements **DROP PROCEDURE IF EXISTS** and **DROP FUNCTION IF EXISTS** were not written to the binary log if the procedure or function to be dropped did not exist. (Bug #13684)

References: See also: Bug #25705.

- Use of **HANDLER** statements with **INFORMATION_SCHEMA** tables caused a server crash. Now **HANDLER** is prohibited with such tables. (Bug #44151)
- `myisamchk` could display a negative `Max keyfile length` value. (Bug #43950)
- `mysqld_multi` incorrectly passed `--no-defaults` to `mysqld_safe`. (Bug #43876)
- On Windows, a server crash occurred for attempts to insert a floating-point value into a **CHAR** column with a maximum length less than the converted floating-point value length. (Bug #43833)
- **UNION** of floating-point numbers did unnecessary rounding. (Bug #43432)
- Certain statements might open a table and then wait for an impending global read lock without noticing whether they hold a table being waiting for by the global read lock, causing a hang. Affected statements are **SELECT ... FOR UPDATE**, **LOCK TABLES ... WRITE**, **TRUNCATE TABLE**, and **LOAD DATA INFILE**. (Bug #43230)
- The InnoDB `btr_search_drop_page_hash_when_freed()` function had a race condition. (Bug #42279)
- Compressing a table with the `myisampack` utility caused the server to produce Valgrind warnings when it opened the table. (Bug #41541)
- For a **MyISAM** table with **DELAY_KEY_WRITE** enabled, the index file could be corrupted without the table being marked as crashed if the server was killed. (Bug #41330)
- Multiple-table **UPDATE** statements did not properly activate triggers. (Bug #39953)
- The functions listed in [MySQL-Specific Functions That Create Geometry Values](#), previously accepted WKB arguments and returned WKB values. They now accept WKB or geometry arguments and return geometry values.

The functions listed in [Functions That Create Geometry Values from WKB Values](#), previously accepted WKB arguments and returned geometry values. They now accept WKB or geometry arguments and return geometry values. (Bug #38990)

- An **UPDATE** statement that updated a column using the same `DES_ENCRYPT()` value for each row actually updated different rows with different values. (Bug #35087)

- For shared-memory connections, the read and write methods did not properly handle asynchronous close events, which could lead to the client locking up waiting for a server response. For example, a call to `mysql_real_query()` would block forever on the client side if the executed statement was aborted on the server side. Thanks to Armin Schöffmann for the bug report and patch. (Bug #33899)
- `CHECKSUM TABLE` was not killable with `KILL QUERY`. (Bug #33146)
- `myisamchk` and `myisampack` were not being linked with the library that enabled support for `*` file name pattern expansion. (Bug #29248)
- `COMMIT` did not delete savepoints if there were no changes in the transaction. (Bug #26288)
- Several memory allocation functions were not being checked for out-of-memory return values. (Bug #25058)

Changes in MySQL Community Server 5.0.81 (2009-05-01)

This is a bugfix release for the current MySQL Community Server production release family. It replaces MySQL 5.0.77.

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- **Performance:** The query cache now checks whether a `SELECT` statement begins with `SQL_NO_CACHE` to determine whether it can skip checking for the query result in the query cache. This is not supported when `SQL_NO_CACHE` occurs within a comment. (Bug #37416)
- The MD5 algorithm now uses the Xfree implementation. (Bug #42434)
- The `libedit` library was upgraded to version 2.11. (Bug #42433)

Bugs Fixed

- **Performance:** For an InnoDB table, `DROP TABLE` or `ALTER TABLE ... DISCARD TABLESPACE` could take a long time or cause a server crash. (Bug #39939)
- **Important Change:** When installing MySQL on Windows, it was possible to install multiple editions (Complete, and Essential, for example) of the same version of MySQL, leading to two separate entries in the installed packages which were impossible to isolate. This could lead to problems with installation and uninstallation. The MySQL installer on Windows no longer permits multiple installations of the same version of MySQL on a single machine. (Bug #4217)
- **MySQL Cluster; Packaging:** Packages for MySQL Cluster were missing the `libndbclient.so` and `libndbclient.a` files. (Bug #42278)
- **Replication:** An `INSERT DELAYED` into a `TIMESTAMP` column issued concurrently with an insert on the same column not using `DELAYED`, but applied after the other insert, was logged using the same timestamp as generated by the other (non-`DELAYED`) insert. (Bug #41719)
- **Replication:** Server IDs greater than 2147483647 ($2^{32} - 1$) were represented by negative numbers in the binary log. (Bug #37313)
- **Replication:** The `--replicate-*-table` options were not evaluated correctly when replicating multi-table updates.

As a result of this fix, replication of multi-table updates no longer fails when an update references a missing table but does not update any of its columns. (Bug #37051)

- **Replication:** When its disk becomes full, a replication slave may wait while writing the binary log, relay log or [MyISAM](#) tables, continuing after space has been made available. The error message provided in such cases was not clear about the frequency with which checking for free space is done (once every 60 seconds), and how long the server waits after space has been freed before continuing (also 60 seconds); this caused users to think that the server had hung.

These issues have been addressed by making the error message clearer, and dividing it into two separate messages:

1. The error message `Disk is full writing 'filename' (Errcode: error_code). Waiting for someone to free space... (Expect up to 60 secs delay for server to continue after freeing disk space)` is printed only once.
2. The warning `Retry in 60 secs, Message reprinted in 600 secs` is printed once every for every 10 times that the check for free space is made; that is, the check is performed once each 60 seconds, but the reminder that space needs to be freed is printed only once every 10 minutes (600 seconds).

(Bug #22082)

- An attempt by a user who did not have the [SUPER](#) privilege to kill a system thread could cause a server crash. (Bug #43748)
- Use of [USE INDEX](#) hints could cause [EXPLAIN EXTENDED](#) to crash. (Bug #43354)
- `mysql` crashed if a request for the current database name returned an empty result, such as after the client has executed a preceding `SET sql_select_limit=0` statement. (Bug #43254)
- On 32-bit Windows, `mysqld` could not use large buffers due to a 2GB user mode address limit. (Bug #43082)
- The `strings/CHARSET_INFO.txt` file was not included in source distributions. (Bug #42937)
- The use by `libedit` of the `__weak_reference()` macro caused compilation failure on FreeBSD. (Bug #42817)
- `mysqldump` included views that were excluded with the `--ignore-table` option. (Bug #42635)
- An optimization introduced for Bug #37553 required an explicit cast to be added for some uses of `TIMEDIFF()` because automatic casting could produce incorrect results. (It was necessary to use `TIME(TIMEDIFF(...))`.) (Bug #42525)

References: See also: Bug #37553.

- Passing an unknown time zone specification to `CONVERT_TZ()` resulted in a memory leak. (Bug #42502)
- Tables could enter open table cache for a thread without being properly cleaned up, leading to a server crash. (Bug #42419)
- The MySQL Instance Configuration Wizard failed to start correctly on Windows Vista. (Bug #42386)
- The SSL certificates included with MySQL distributions were regenerated because the previous ones had expired. (Bug #42366)

- Dependent subqueries such as the following caused a memory leak proportional to the number of outer rows:

```
SELECT COUNT(*) FROM t1, t2 WHERE t2.b
  IN (SELECT DISTINCT t2.b FROM t2 WHERE t2.b = t1.a);
```

(Bug #42037)

- `mysqldumpslow` parsed the `--debug` and `--verbose` options incorrectly. (Bug #42027)
- Some queries using `NAME_CONST(.. COLLATE ...)` led to a server crash due to a failed type cast. (Bug #42014)
- On Mac OS X, some of the universal client libraries were not actually universal and were missing code for one or more architectures. (Bug #41940)
- String reallocation could cause memory overruns. (Bug #41868)
- With more than two arguments, `LEAST()`, `GREATEST()`, and `CASE` could unnecessarily return `Illegal mix of collations` errors. (Bug #41627)
- Queries that used the loose index scan access method could return no rows. (Bug #41610)
- In `InnoDB` recovery after a server crash, rollback of a transaction that updated a column from `NULL` to `NULL` could cause another crash. (Bug #41571)
- If `InnoDB` reached its limit on the number of concurrent transactions (1023), it wrote a descriptive message to the error log but returned a misleading error message to the client, or an assertion failure occurred. (Bug #41529)
- The `mysql` client could misinterpret its input if a line was longer than an internal buffer. (Bug #41486)
- `DATE_FORMAT()` could cause a server crash for year-zero dates. (Bug #41470)
- When substituting system constant functions with a constant result, the server was not expecting `NULL` function return values and could crash. (Bug #41437)
- For a `TIMESTAMP NOT NULL DEFAULT ...` column, storing `NULL` as the return value from some functions caused a “cannot be NULL” error. `NULL` returns now correctly cause the column default value to be stored. (Bug #41370)
- Use of `SELECT *` permitted users with rights to only some columns of a view to access all columns. (Bug #41354)
- In the `help` command output displayed by `mysql`, the description for the `\c` (`clear`) command was misleading. (Bug #41268)
- The server did not robustly handle problems hang if a table opened with `HANDLER` needed to be re-opened because it had been altered to use a different storage engine that does not support `HANDLER`. The server also failed to set an error if the re-open attempt failed. These problems could cause the server to crash or hang. (Bug #41110, Bug #41112)
- For prepared statements, multibyte character sets were not taking into account when calculating `max_length` for string values and `mysql_stmt_fetch()` could return truncated strings. (Bug #41078)
- The Windows installer displayed incorrect product names in some images. (Bug #40845)
- The `mysql_change_user()` C API function changed the value of the `sql_big_selects` session variable. (Bug #40363)

References: See also: Bug #20023.

- For a view that references a table in another database, `mysqldump` wrote the view name qualified with the current database name. This makes it impossible to reload the dump file into a different database. (Bug #40345)
- The query cache stored only partial query results if a statement failed while the results were being sent to the client. This could cause other clients to hang when trying to read the cached result. Now if a statement fails, the result is not cached. (Bug #40264)
- `perror` did not produce correct output for error codes 153 to 163. (Bug #39370)
- The expression `ROW(...) IN (SELECT ... FROM DUAL)` always returned `TRUE`. (Bug #39069)
- The greedy optimizer could cause a server crash due to improper handling of nested outer joins. (Bug #38795)
- Use of `COUNT(DISTINCT)` prevented `NULL` testing in the `HAVING` clause. (Bug #38637)
- When running the MySQL Instance Configuration Wizard in command-line only mode, the service name would be ignored (effectively creating all instances with the default `MySQL` service name), irrespective of the name specified on the command line. However, the wizard would attempt to start the service with the specified name, and failed. (Bug #38379)
- Enabling the `sync_frm` system variable had no effect on the handling of `.frm` files for views. (Bug #38145)
- Comparisons between row constructors, such as `(a, b) = (c, d)` resulted in unnecessary `Illegal mix of collations` errors for string columns. (Bug #37601)
- An argument to the `MATCH()` function that was an alias for an expression other than a column name caused a server crash. (Bug #36737)
- The query cache stored packets containing the server status of the time when the cached statement was run. This might lead to an incorrect transaction status on the client side if a statement was cached during a transaction and later served outside a transaction context (or vice versa). (Bug #36326)
- If the system time was adjusted backward during query execution, the apparent execution time could be negative. But in some cases these queries would be written to the slow query log, with the negative execution time written as a large unsigned number. Now statements with apparent negative execution time are not written to the slow query log. (Bug #35396)
- The use of `NAME_CONST()` can result in a problem for `CREATE TABLE ... SELECT` statements when the source column expressions refer to local variables. Converting these references to `NAME_CONST()` expressions can result in column names that are different on the master and slave servers, or names that are too long to be legal column identifiers. A workaround is to supply aliases for columns that refer to local variables.

Now a warning is issued in such cases that indicate possible problems. (Bug #35383)

- For `DROP FUNCTION` with names that were qualified with a database name, the database name was handled in case-sensitive fashion even with `lower_case_table_names` set to 1. (Bug #33813)
- `mysqldump --compatible=mysql40` emitted statements referring to the `character_set_client` system variable, which is unknown before MySQL 4.1. Now the statements are enclosed in version-specific comments. (Bug #33550)

- For `mysqld_multi`, using the `--mysqld=mysqld_safe` option caused the `--defaults-file` and `--defaults-extra-file` options to behave the same way. (Bug #32136)
- Attempts to open a valid `MERGE` table sometimes resulted in a `ER_WRONG_MRG_TABLE` error. This happened after failure to open an invalid `MERGE` table had also generated an `ER_WRONG_MRG_TABLE` error. (Bug #32047)
- Use of MBR spatial functions such as `MBRTouches()` with columns of `InnoDB` tables caused a server crash rather than an error. (Bug #31435)
- The `mysql_change_user()` C API function caused global `Com_xxx` status variable values to be incorrect. (Bug #31222)
- For Solaris package installation using `pkgadd`, the postinstall script failed, causing the system tables in the `mysql` database not to be created. (Bug #31164)
- The `mysql` client mishandled input parsing if a `delimiter` command was not first on the line. (Bug #31060)
- For installation on Solaris using `pkgadd` packages, the `mysql_install_db` script was generated in the `scripts` directory, but the temporary files used during the process were left there and not deleted. (Bug #31052)
- `SHOW PRIVILEGES` listed the `CREATE ROUTINE` privilege as having a context of `Functions, Procedures`, but it is a database-level privilege. (Bug #30305)
- `CHECK TABLE`, `REPAIR TABLE`, `ANALYZE TABLE`, and `OPTIMIZE TABLE` erroneously reported a table to be corrupt if the table did not exist or the statement was terminated with `KILL`. (Bug #29458)
- When installing the Windows service, using quotation marks around command-line configuration parameters could cause the quotation marks to be incorrectly placed around the entire command-line option, and not just the value. (Bug #27535)
- `SHOW TABLE STATUS` could fail to produce output for tables with non-ASCII characters in their name. (Bug #25830)
- The `Time` column for `SHOW PROCESSLIST` output now can have negative values. Previously, the column was unsigned and negative values were displayed incorrectly as large positive values. Negative values can occur if a thread alters the time into the future with `SET TIMESTAMP = value` or the thread is executing on a slave and processing events from a master that has its clock set ahead of the slave. (Bug #22047)
- Restoring a `mysqldump` dump file containing `FEDERATED` tables failed because the file contained the data for the table. Now only the table definition is dumped (because the data is located elsewhere). (Bug #21360)
- Floating-point numbers could be handled with different numbers of digits depending on whether the text or prepared-statement protocol was used. (Bug #21205)
- Incorrect length metadata could be returned for `LONG TEXT` columns when a multibyte server character set was used. (Bug #19829)
- `ROUND()` sometimes returned different results on different platforms. (Bug #15936)

Changes in MySQL Enterprise 5.0.80 [MRU] (2009-05-01)

This is a *Monthly Rapid Update* release of the MySQL Enterprise Server 5.0.

This section documents all changes and bugfixes that have been applied since the last MySQL Enterprise Server release (5.0.79). If you would like to receive more fine-grained and personalized *update alerts* about fixes that are relevant to the version and features you use, please consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details please see <http://www.mysql.com/products/enterprise/advisors.html>.

Support Ending for AIX 5.2: Per the <http://www.mysql.com/about/legal/lifecycle/> regarding ending support for OS versions that have reached vendor end of life, we plan to discontinue building or supporting MySQL binaries for AIX 5.2 as of April 30, 2009. This release of MySQL 5.0 (5.0.80) is the last MySQL 5.0 release with support for AIX 5.2. For more information, see the March 24, 2009 note at [MySQL Product Support EOL Announcements](#).

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- The MD5 algorithm now uses the Xfree implementation. (Bug #42434)

Bugs Fixed

- **Replication:** An `INSERT DELAYED` into a `TIMESTAMP` column issued concurrently with an insert on the same column not using `DELAYED`, but applied after the other insert, was logged using the same timestamp as generated by the other (non-`DELAYED`) insert. (Bug #41719)
- An attempt by a user who did not have the `SUPER` privilege to kill a system thread could cause a server crash. (Bug #43748)
- Use of `USE INDEX` hints could cause `EXPLAIN EXTENDED` to crash. (Bug #43354)
- `mysql` crashed if a request for the current database name returned an empty result, such as after the client has executed a preceding `SET sql_select_limit=0` statement. (Bug #43254)
- The `strings/CHARSET_INFO.txt` file was not included in source distributions. (Bug #42937)
- `mysqldump` included views that were excluded with the `--ignore-table` option. (Bug #42635)
- Passing an unknown time zone specification to `CONVERT_TZ()` resulted in a memory leak. (Bug #42502)
- The MySQL Instance Configuration Wizard failed to start correctly on Windows Vista. (Bug #42386)
- With more than two arguments, `LEAST()`, `GREATEST()`, and `CASE` could unnecessarily return `Illegal mix of collations` errors. (Bug #41627)
- The `mysql` client could misinterpret its input if a line was longer than an internal buffer. (Bug #41486)
- In the `help` command output displayed by `mysql`, the description for the `\c (clear)` command was misleading. (Bug #41268)
- When running the MySQL Instance Configuration Wizard in command-line only mode, the service name would be ignored (effectively creating all instances with the default `MySQL` service name), irrespective of the name specified on the command line. However, the wizard would attempt to start the service with the specified name, and failed. (Bug #38379)
- The use of `NAME_CONST()` can result in a problem for `CREATE TABLE ... SELECT` statements when the source column expressions refer to local variables. Converting these references to `NAME_CONST()` expressions can result in column names that are different on the master and slave servers, or names

that are too long to be legal column identifiers. A workaround is to supply aliases for columns that refer to local variables.

Now a warning is issued in such cases that indicate possible problems. (Bug #35383)

- `CHECK TABLE`, `REPAIR TABLE`, `ANALYZE TABLE`, and `OPTIMIZE TABLE` erroneously reported a table to be corrupt if the table did not exist or the statement was terminated with `KILL`. (Bug #29458)
- The `Time` column for `SHOW PROCESSLIST` output now can have negative values. Previously, the column was unsigned and negative values were displayed incorrectly as large positive values. Negative values can occur if a thread alters the time into the future with `SET TIMESTAMP = value` or the thread is executing on a slave and processing events from a master that has its clock set ahead of the slave. (Bug #22047)
- Restoring a `mysqldump` dump file containing `FEDERATED` tables failed because the file contained the data for the table. Now only the table definition is dumped (because the data is located elsewhere). (Bug #21360)

Changes in MySQL Enterprise 5.0.79 [MRU] (2009-03-09)

This is a *Monthly Rapid Update* release of the MySQL Enterprise Server 5.0.

This section documents all changes and bugfixes that have been applied since the last MySQL Enterprise Server release (5.0.78). If you would like to receive more fine-grained and personalized *update alerts* about fixes that are relevant to the version and features you use, please consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details please see <http://www.mysql.com/products/enterprise/advisors.html>.

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- **Performance:** The query cache now checks whether a `SELECT` statement begins with `SQL_NO_CACHE` to determine whether it can skip checking for the query result in the query cache. This is not supported when `SQL_NO_CACHE` occurs within a comment. (Bug #37416)
- The `libedit` library was upgraded to version 2.11. (Bug #42433)

Bugs Fixed

- **Performance:** For an `InnoDB` table, `DROP TABLE` or `ALTER TABLE ... DISCARD TABLESPACE` could take a long time or cause a server crash. (Bug #39939)
- **Replication:** Server IDs greater than 2147483647 ($2^{32} - 1$) were represented by negative numbers in the binary log. (Bug #37313)
- **Replication:** The `--replicate-*-table` options were not evaluated correctly when replicating multi-table updates.

As a result of this fix, replication of multi-table updates no longer fails when an update references a missing table but does not update any of its columns. (Bug #37051)

- **Replication:** When its disk becomes full, a replication slave may wait while writing the binary log, relay log or `MyISAM` tables, continuing after space has been made available. The error message provided in such cases was not clear about the frequency with which checking for free space is done (once every

60 seconds), and how long the server waits after space has been freed before continuing (also 60 seconds); this caused users to think that the server had hung.

These issues have been addressed by making the error message clearer, and dividing it into two separate messages:

1. The error message `Disk is full writing 'filename' (Errcode: error_code). Waiting for someone to free space... (Expect up to 60 secs delay for server to continue after freeing disk space)` is printed only once.
2. The warning `Retry in 60 secs, Message reprinted in 600 secs` is printed once every for every 10 times that the check for free space is made; that is, the check is performed once each 60 seconds, but the reminder that space needs to be freed is printed only once every 10 minutes (600 seconds).

(Bug #22082)

- On 32-bit Windows, `mysqld` could not use large buffers due to a 2GB user mode address limit. (Bug #43082)
- The use by `libedit` of the `__weak_reference()` macro caused compilation failure on FreeBSD. (Bug #42817)
- Tables could enter open table cache for a thread without being properly cleaned up, leading to a server crash. (Bug #42419)
- `mysqldumpslow` parsed the `--debug` and `--verbose` options incorrectly. (Bug #42027)
- String reallocation could cause memory overruns. (Bug #41868)
- Queries that used the loose index scan access method could return no rows. (Bug #41610)
- In `InnoDB` recovery after a server crash, rollback of a transaction that updated a column from `NULL` to `NULL` could cause another crash. (Bug #41571)
- If `InnoDB` reached its limit on the number of concurrent transactions (1023), it wrote a descriptive message to the error log but returned a misleading error message to the client, or an assertion failure occurred. (Bug #41529)
- Use of `SELECT *` permitted users with rights to only some columns of a view to access all columns. (Bug #41354)
- The server did not robustly handle problems hang if a table opened with `HANDLER` needed to be re-opened because it had been altered to use a different storage engine that does not support `HANDLER`. The server also failed to set an error if the re-open attempt failed. These problems could cause the server to crash or hang. (Bug #41110, Bug #41112)
- For prepared statements, multibyte character sets were not taking into account when calculating `max_length` for string values and `mysql_stmt_fetch()` could return truncated strings. (Bug #41078)
- The `mysql_change_user()` C API function changed the value of the `sql_big_selects` session variable. (Bug #40363)

References: See also: Bug #20023.

- For a view that references a table in another database, `mysqldump` wrote the view name qualified with the current database name. This makes it impossible to reload the dump file into a different database. (Bug #40345)

- `perror` did not produce correct output for error codes 153 to 163. (Bug #39370)
- Comparisons between row constructors, such as `(a, b) = (c, d)` resulted in unnecessary `Illegal mix of collations` errors for string columns. (Bug #37601)
- An argument to the `MATCH()` function that was an alias for an expression other than a column name caused a server crash. (Bug #36737)
- For `DROP FUNCTION` with names that were qualified with a database name, the database name was handled in case-sensitive fashion even with `lower_case_table_names` set to 1. (Bug #33813)
- `mysqldump --compatible=mysql40` emitted statements referring to the `character_set_client` system variable, which is unknown before MySQL 4.1. Now the statements are enclosed in version-specific comments. (Bug #33550)
- Use of MBR spatial functions such as `MBRTouches()` with columns of InnoDB tables caused a server crash rather than an error. (Bug #31435)
- The `mysql` client mishandled input parsing if a `delimiter` command was not first on the line. (Bug #31060)
- For installation on Solaris using `pkgadd` packages, the `mysql_install_db` script was generated in the `scripts` directory, but the temporary files used during the process were left there and not deleted. (Bug #31052)
- `SHOW PRIVILEGES` listed the `CREATE ROUTINE` privilege as having a context of `Functions, Procedures`, but it is a database-level privilege. (Bug #30305)
- `SHOW TABLE STATUS` could fail to produce output for tables with non-ASCII characters in their name. (Bug #25830)
- Floating-point numbers could be handled with different numbers of digits depending on whether the text or prepared-statement protocol was used. (Bug #21205)
- Incorrect length metadata could be returned for `LONG TEXT` columns when a multibyte server character set was used. (Bug #19829)
- `ROUND()` sometimes returned different results on different platforms. (Bug #15936)

Changes in MySQL Enterprise 5.0.78 [MRU] (2009-02-06)

This is a *Monthly Rapid Update* release of the MySQL Enterprise Server 5.0.

This section documents all changes and bugfixes that have been applied since the last MySQL Enterprise Server release (5.0.76). If you would like to receive more fine-grained and personalized *update alerts* about fixes that are relevant to the version and features you use, please consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details please see <http://www.mysql.com/products/enterprise/advisors.html>.

Bugs Fixed

- **Important Change:** When installing MySQL on Windows, it was possible to install multiple editions (Complete, and Essential, for example) of the same version of MySQL, leading to two separate entries in the installed packages which were impossible to isolate. This could lead to problems with installation and uninstallation. The MySQL installer on Windows no longer permits multiple installations of the same version of MySQL on a single machine. (Bug #4217)
- **MySQL Cluster; Packaging:** Packages for MySQL Cluster were missing the `libndbclient.so` and `libndbclient.a` files. (Bug #42278)

- An optimization introduced for Bug #37553 required an explicit cast to be added for some uses of `TIMEDIFF()` because automatic casting could produce incorrect results. (It was necessary to use `TIME(TIMEDIFF(...))`.) (Bug #42525)

References: See also: Bug #37553.

- The SSL certificates included with MySQL distributions were regenerated because the previous ones had expired. (Bug #42366)
- Dependent subqueries such as the following caused a memory leak proportional to the number of outer rows:

```
SELECT COUNT(*) FROM t1, t2 WHERE t2.b
  IN (SELECT DISTINCT t2.b FROM t2 WHERE t2.b = t1.a);
```

(Bug #42037)

- Some queries using `NAME_CONST(... COLLATE ...)` led to a server crash due to a failed type cast. (Bug #42014)
- On Mac OS X, some of the universal client libraries were not actually universal and were missing code for one or more architectures. (Bug #41940)
- `DATE_FORMAT()` could cause a server crash for year-zero dates. (Bug #41470)
- When substituting system constant functions with a constant result, the server was not expecting `NULL` function return values and could crash. (Bug #41437)
- For a `TIMESTAMP NOT NULL DEFAULT ...` column, storing `NULL` as the return value from some functions caused a "cannot be NULL" error. `NULL` returns now correctly cause the column default value to be stored. (Bug #41370)
- The Windows installer displayed incorrect product names in some images. (Bug #40845)
- The query cache stored only partial query results if a statement failed while the results were being sent to the client. This could cause other clients to hang when trying to read the cached result. Now if a statement fails, the result is not cached. (Bug #40264)
- The expression `ROW(...) IN (SELECT ... FROM DUAL)` always returned `TRUE`. (Bug #39069)
- The greedy optimizer could cause a server crash due to improper handling of nested outer joins. (Bug #38795)
- Use of `COUNT(DISTINCT)` prevented `NULL` testing in the `HAVING` clause. (Bug #38637)
- Enabling the `sync_frm` system variable had no effect on the handling of `.frm` files for views. (Bug #38145)
- The query cache stored packets containing the server status of the time when the cached statement was run. This might lead to an incorrect transaction status on the client side if a statement was cached during a transaction and later served outside a transaction context (or vice versa). (Bug #36326)
- If the system time was adjusted backward during query execution, the apparent execution time could be negative. But in some cases these queries would be written to the slow query log, with the negative execution time written as a large unsigned number. Now statements with apparent negative execution time are not written to the slow query log. (Bug #35396)
- For `mysqld_multi`, using the `--mysqld=mysqld_safe` option caused the `--defaults-file` and `--defaults-extra-file` options to behave the same way. (Bug #32136)

- Attempts to open a valid `MERGE` table sometimes resulted in a `ER_WRONG_MRG_TABLE` error. This happened after failure to open an invalid `MERGE` table had also generated an `ER_WRONG_MRG_TABLE` error. (Bug #32047)
- The `mysql_change_user()` C API function caused global `Com_xxx` status variable values to be incorrect. (Bug #31222)
- For Solaris package installation using `pkgadd`, the postinstall script failed, causing the system tables in the `mysql` database not to be created. (Bug #31164)
- When installing the Windows service, using quotation marks around command-line configuration parameters could cause the quotation marks to be incorrectly placed around the entire command-line option, and not just the value. (Bug #27535)

Changes in MySQL Community Server 5.0.77 (2009-01-28)

This is a bugfix release for the current MySQL Community Server production release family. It replaces MySQL 5.0.67 (binary) and 5.0.75 (source-only).

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- **Security Enhancement:** To enable stricter control over the location from which user-defined functions can be loaded, the `plugin_dir` system variable has been backported from MySQL 5.1. If the value is nonempty, user-defined function object files can be loaded only from the directory named by this variable. If the value is empty, the behavior that is used prior to the inclusion of `plugin_dir` applies: The UDF object files must be located in a directory that is searched by your system's dynamic linker.

If the plugin directory is writable by the server, it may be possible for a user to write executable code to a file in the directory using `SELECT ... INTO DUMPFILE`. This can be prevented by making `plugin_dir` read only to the server or by setting `--secure-file-priv` to a directory where `SELECT` writes can be made safely. (Bug #37428)

- A new status variable, `Queries`, indicates the number of statements executed by the server. This includes statements executed within stored programs, unlike the `Questions` variable which includes only statements sent to the server by clients. (Bug #41131)
- Previously, index hints did not work for `FULLTEXT` searches. Now they work as follows:

For natural language mode searches, index hints are silently ignored. For example, `IGNORE INDEX(i)` is ignored with no warning and the index is still used.

For boolean mode searches, index hints are honored. (Bug #38842)

Bugs Fixed

- **Security Fix; Important Change:** Additional corrections were made for the symlink-related privilege problem originally addressed in MySQL 5.0.60. The original fix did not correctly handle the data directory path name if it contained symlinked directories in its path, and the check was made only at table-creation time, not at table-opening time later. (Bug #32167, CVE-2008-2079)

References: See also: Bug #39277.

- **Security Enhancement:** The server consumed excess memory while parsing statements with hundreds or thousands of nested boolean conditions (such as `OR (OR ... (OR ...))`). This could lead to

a server crash or incorrect statement execution, or cause other client statements to fail due to lack of memory. The latter result constitutes a denial of service. (Bug #38296)

- **Incompatible Change:** There were some problems using `DllMain()` hook functions on Windows that automatically do global and per-thread initialization for `libmysqld.dll`:
 - Per-thread initialization: MySQL internally counts the number of active threads, which causes a delay in `my_end()` if not all threads have exited. But there are threads that can be started either by Windows internally (often in TCP/IP scenarios) or by users. Those threads do not necessarily use `libmysqld.dll` functionality but still contribute to the open-thread count. (One symptom is a five-second delay in times for PHP scripts to finish.)
 - Process-initialization: `my_init()` calls `WSAStartup` that itself loads DLLs and can lead to a deadlock in the Windows loader.

To correct these problems, DLL initialization code now is not invoked from `libmysqld.dll` by default. To obtain the previous behavior (DLL initialization code will be called), set the `LIBMYSQL_DLLINIT` environment variable to any value. This variable exists only to prevent breakage of existing Windows-only applications that do not call `mysql_thread_init()` and work okay today. Use of `LIBMYSQL_DLLINIT` is discouraged and is removed in MySQL 6.0. (Bug #37226, Bug #33031)

- **Incompatible Change:** `SHOW STATUS` took a lot of CPU time for calculating the value of the `InnoDB_buffer_pool_pages_latched` status variable. Now this variable is calculated and included in the output of `SHOW STATUS` only if the `UNIV_DEBUG` symbol is defined at MySQL build time. (Bug #36600)
- **Incompatible Change:** In connection with view creation, the server created `arc` directories inside database directories and maintained useless copies of `.frm` files there. Creation and renaming procedures of those copies as well as creation of `arc` directories has been discontinued.

This change does cause a problem when downgrading to older server versions which manifests itself under these circumstances:

1. Create a view `v_orig` in MySQL 5.0.72 or higher.
2. Rename the view to `v_new` and then back to `v_orig`.
3. Downgrade to an older 5.0.x server and run `mysql_upgrade`.
4. Try to rename `v_orig` to `v_new` again. This operation fails.

As a workaround to avoid this problem, use either of these approaches:

- Dump your data using `mysqldump` before downgrading and reload the dump file after downgrading.
- Instead of renaming a view after the downgrade, drop it and recreate it.

The downgrade problem introduced by the fix for this bug has been addressed as Bug #40021. (Bug #17823)

References: See also: Bug #40021.

- **Replication:** When rotating relay log files, the slave deletes relay log files and then edits the relay log index file. Formerly, if the slave shut down unexpectedly between these two events, the relay log index file could then reference relay logs that no longer existed. Depending on the circumstances, this could when restarting the slave cause either a race condition or the failure of replication. (Bug #38826, Bug #39325)

- In example option files provided in MySQL distributions, the `thread_stack` value was increased from 64K to 128K. (Bug #41577)
- `SET PASSWORD` caused a server crash if the account name was given as `CURRENT_USER()`. (Bug #41456)
- The `INFORMATION_SCHEMA.SCHEMA_PRIVILEGES` table was limited to 7680 rows. (Bug #41079)
- In debug builds, obsolete debug code could be used to crash the server. (Bug #41041)
- `CHECK TABLE ... FOR UPGRADE` did not check for incompatible collation changes made in MySQL 5.0.48 (Bug #27562, Bug #29461, Bug #29499). This also affects `mysqlcheck` and `mysql_upgrade`, which cause that statement to be executed. See [Checking Whether Tables or Indexes Must Be Rebuilt](#). (Bug #40984)

References: See also: Bug #39585, Bug #27562, Bug #29461, Bug #29499.

- Some queries that used a “range checked for each record” scan could return incorrect results. (Bug #40974)

References: See also: Bug #44810.

- Certain `SELECT` queries could fail with a `Duplicate entry` error. (Bug #40953)
- The `FEDERATED` handler had a memory leak. (Bug #40875)
- `IF(..., CAST(longtext_val AS UNSIGNED), signed_val)` as an argument to an aggregate function could cause an assertion failure. (Bug #40761)
- Prepared statements permitted invalid dates to be inserted when the `ALLOW_INVALID_DATES` SQL mode was not enabled. (Bug #40365)
- `mc.exe` is no longer needed to compile MySQL on Windows. This makes it possible to build MySQL from source using Visual Studio Express 2008. (Bug #40280)
- Support for the `revision` field in `.frm` files has been removed. This addresses the downgrading problem introduced by the fix for Bug #17823. (Bug #40021)

References: See also: Bug #17823.

- If the operating system is configured to return leap seconds from OS time calls or if the MySQL server uses a time zone definition that has leap seconds, functions such as `NOW()` could return a value having a time part that ends with `:59:60` or `:59:61`. If such values are inserted into a table, they would be dumped as is by `mysqldump` but considered invalid when reloaded, leading to backup/restore problems.

Now leap second values are returned with a time part that ends with `:59:59`. This means that a function such as `NOW()` can return the same value for two or three consecutive seconds during the leap second. It remains true that literal temporal values having a time part that ends with `:59:60` or `:59:61` are considered invalid.

For additional details about leap-second handling, see [Time Zone Leap Second Support](#). (Bug #39920)

- The server could crash during a sort-order optimization of a dependent subquery. (Bug #39844)
- With the `ONLY_FULL_GROUP_BY` SQL mode enabled, the check for nonaggregated columns in queries with aggregate functions, but without a `GROUP BY` clause was treating all the parts of the query as if they were in the select list. This is fixed by ignoring the nonaggregated columns in the `WHERE` clause. (Bug #39656)

- The server crashed if an integer field in a CSV file did not have delimiting quotation marks. (Bug #39616)
- Creating a table with a comment of 62 characters or longer caused a server crash. (Bug #39591)
- `CHECK TABLE` failed for `MyISAM INFORMATION_SCHEMA` tables. (Bug #39541)
- `InnoDB` could hang trying to open an adaptive hash index. (Bug #39483)
- For a `TIMESTAMP` column in an `InnoDB` table, testing the column with multiple conditions in the `WHERE` clause caused a server crash. (Bug #39353)
- The server returned a column type of `VARBINARY` rather than `DATE` as the result from the `COALESCE()`, `IFNULL()`, `IF()`, `GREATEST()`, or `LEAST()` functions or `CASE` expression if the result was obtained using `filesort` in an anonymous temporary table during the query execution. (Bug #39283)
- References to local variables in stored procedures are replaced with `NAME_CONST(name, value)` when written to the binary log. However, an “illegal mix of collation” error might occur when executing the log contents if the value's collation differed from that of the variable. Now information about the variable collation is written as well. (Bug #39182)
- Some recent releases for Solaris 10 were built on Solaris 10 U5, which included a new version of `libnsl.so` that does not work on U4 or earlier. To correct this, Solaris 10 builds now are created on machines that do not have that upgraded `libnsl.so`, so that they will work on Solaris 10 installations both with and without the upgraded `libnsl.so`. (Bug #39074)
- With binary logging enabled `CREATE VIEW` was subject to possible buffer overwrite and a server crash. (Bug #39040)
- Queries of the form `SELECT ... REGEXP BINARY NULL` could lead to a hung or crashed server. (Bug #39021)
- Statements of the form `INSERT ... SELECT .. ON DUPLICATE KEY UPDATE col_name = DEFAULT` could result in a server crash. (Bug #39002)
- Column names constructed due to wild-card expansion done inside a stored procedure could point to freed memory if the expansion was performed after the first call to the stored procedure. (Bug #38823)
- Repeated `CREATE TABLE ... SELECT` statements, where the created table contained an `AUTO_INCREMENT` column, could lead to an assertion failure. (Bug #38821)
- If delayed insert failed to upgrade the lock, it did not free the temporary memory storage used to keep newly constructed `BLOB` values in memory, resulting in a memory leak. (Bug #38693)
- A server crash resulted from concurrent execution of a multiple-table `UPDATE` that used a `NATURAL` or `USING` join together with `FLUSH TABLES WITH READ LOCK` or `ALTER TABLE` for the table being updated. (Bug #38691)
- On ActiveState Perl, `mysql-test-run.pl --start-and-exit` started but did not exit. (Bug #38629)
- Server-side cursors were not initialized properly, which could cause a server crash. (Bug #38486)
- Stored procedures involving substrings could crash the server on certain platforms due to invalid memory reads. (Bug #38469)
- A server crash or Valgrind warnings could result when a stored procedure selected from a view that referenced a function. (Bug #38291)

- Incorrect handling of aggregate functions when loose index scan was used caused a server crash. (Bug #38195)
- Queries containing a subquery with `DISTINCT` and `ORDER BY` could cause a server crash. (Bug #38191)
- Queries with a `HAVING` clause could return a spurious row. (Bug #38072)
- Use of spatial data types in prepared statements could cause memory leaks or server crashes. (Bug #37956, Bug #37671)
- The server crashed if an argument to a stored procedure was a subquery that returned more than one row. (Bug #37949)
- When analyzing the possible index use cases, the server was incorrectly reusing an internal structure, leading to a server crash. (Bug #37943)
- A `SELECT` with a `NULL NOT IN` condition containing a complex subquery from the same table as in the outer select caused an assertion failure. (Bug #37894)
- For `InnoDB` tables, `ORDER BY ... DESC` sometimes returned results in ascending order. (Bug #37830)
- If a table has a `BIT NOT NULL` column `c1` with a length shorter than 8 bits and some additional `NOT NULL` columns `c2`, ..., and a `SELECT` query has a `WHERE` clause of the form `(c1 = constant) AND c2 ...`, the query could return an unexpected result set. (Bug #37799)
- Nesting of `IF()` inside of `SUM()` could cause an extreme server slowdown. (Bug #37662)
- The `MONTHNAME()` and `DAYNAME()` functions returned a binary string, so that using `LOWER()` or `UPPER()` had no effect. Now `MONTHNAME()` and `DAYNAME()` return a value in `character_set_connection` character set. (Bug #37575)
- `TIMEDIFF()` was erroneously treated as always returning a positive result. Also, `CAST()` of `TIME` values to `DECIMAL` dropped the sign of negative values. (Bug #37553)

References: See also: Bug #42525.

- `mysqlcheck` used `SHOW FULL TABLES` to get the list of tables in a database. For some problems, such as an empty `.frm` file for a table, this failed and `mysqlcheck` then would neglect to check other tables in the database. (Bug #37527)
- The `<=>` operator could return incorrect results when comparing `NULL` to `DATE`, `TIME`, or `DATETIME` values. (Bug #37526)
- Updating a view with a subquery in the `CHECK` option could cause an assertion failure. (Bug #37460)
- Statements that displayed the value of system variables (for example, `SHOW VARIABLES`) expect variable values to be encoded in `character_set_system`. However, variables set from the command line such as `basedir` or `datadir` were encoded using `character_set_filesystem` and not converted correctly. (Bug #37339)
- For a `MyISAM` table with `CHECKSUM = 1` and `ROW_FORMAT = DYNAMIC` table options, a data consistency check (maximum record length) could fail and cause the table to be marked as corrupted. (Bug #37310)
- The `max_length` result set metadata value was calculated incorrectly under some circumstances. (Bug #37301)

- `CREATE INDEX` could crash with `InnoDB` plugin 1.0.1. (Bug #37284)
- Certain boolean-mode `FULLTEXT` searches that used the truncation operator did not return matching records and calculated relevance incorrectly. (Bug #37245)
- The `NO_BACKSLASH_ESCAPES` SQL mode was ignored for `LOAD DATA INFILE` and `SELECT INTO ... OUTFILE`. The setting is taken into account now. (Bug #37114)
- On a 32-bit server built without big tables support, the offset argument in a `LIMIT` clause might be truncated due to a 64-bit to 32-bit cast. (Bug #37075)
- If the server failed to expire binary log files at startup, it could crash. (Bug #37027)
- The code for the `ut_usecetime()` function in `InnoDB` did not handle errors from the `gettimeofday()` system call. Now it retries `gettimeofday()` several times and updates the value of the `InnoDB_row_lock_time_max` status variable only if `ut_usecetime()` was successful. (Bug #36819)
- Use of `CONVERT()` with `GROUP BY` to convert numeric values to `CHAR` could return truncated results. (Bug #36772)
- A query which had an `ORDER BY DESC` clause that is satisfied with a reverse range scan could cause a server crash for some specific CPU/compiler combinations. (Bug #36639)
- Dumping information about locks in use by sending a `SIGHUP` signal to the server or by invoking the `mysqladmin debug` command could lead to a server crash in debug builds or to undefined behavior in production builds. (Bug #36579)
- The `mysql` client, when built with Visual Studio 2005, did not display Japanese characters. (Bug #36279)
- When the fractional part in a multiplication of `DECIMAL` values overflowed, the server truncated the first operand rather than the longest. Now the server truncates so as to produce more precise multiplications. (Bug #36270)
- A read past the end of the string could occur while parsing the value of the `--innodb-data-file-path` option. (Bug #36149)
- Host name values in SQL statements were not being checked for '@', which is illegal according to RFC952. (Bug #35924)
- The `UUID()` function returned UUIDs with the wrong time; this was because the offset for the time part in UUIDs was miscalculated. (Bug #35848)
- `SHOW CREATE TABLE` did not display a printable value for the default value of `BIT` columns. (Bug #35796)
- `mysql_install_db` failed on machines that had the host name set to `localhost`. (Bug #35754)
- Dynamic plugins failed to load on i5/OS. (Bug #35743)
- Freeing of an internal parser stack during parsing of complex stored programs caused a server crash. (Bug #35577, Bug #37269, Bug #37228)
- The `max_length` metadata value was calculated incorrectly for the `FORMAT()` function, which could cause incorrect result set metadata to be sent to clients. (Bug #35558)
- Index scans performed with the `sort_union()` access method returned wrong results, caused memory to be leaked, and caused temporary files to be deleted when the limit set by `sort_buffer_size` was reached. (Bug #35477, Bug #35478)

- If the server crashed with an `InnoDB` error due to unavailability of undo slots, errors could persist during rollback when the server was restarted: There are two `UNDO` slot caches (for `INSERT` and `UPDATE`). If all slots end up in one of the slot caches, a request for a slot from the other slot cache failed. This can happen if the request is for an `UPDATE` slot and all slots are in the `INSERT` slot cache, or vice versa. (Bug #35352)
- For `InnoDB` tables, `ALTER TABLE DROP` failed if the name of the column to be dropped began with “foreign”. (Bug #35220)
- `perror` on Windows did not know about Win32 system error codes. (Bug #34825)
- `EXPLAIN EXTENDED` evaluation of aggregate functions that required a temporary table caused a server crash. (Bug #34773)
- Queries of the form `SELECT ... WHERE string = ANY(...)` failed when the server used a single-byte character set and the client used a multibyte character set. (Bug #34760)

References: See also: Bug #20835.

- Using `OPTIMIZE TABLE` as the first statement on an `InnoDB` table with an `AUTO_INCREMENT` column could cause a server crash. (Bug #34286)
- `mysql_install_db` failed if the server was running with an SQL mode of `TRADITIONAL`. This program now resets the SQL mode internally to avoid this problem. (Bug #34159)
- Changes to build files were made to enable the MySQL distribution to compile on Microsoft Visual C++ Express 2008. (Bug #33907)
- The `mysql` client incorrectly parsed statements containing the word “delimiter” in mid-statement. This fix is different from the one applied for this bug in MySQL 5.0.66. (Bug #33812)

References: See also: Bug #38158.

- For a stored procedure containing a `SELECT * ... RIGHT JOIN` query, execution failed for the second call. (Bug #33811)
- Previously, use of index hints with views (which do not have indexes) produced the error `ERROR 1221 (HY000): Incorrect usage of USE/IGNORE INDEX and VIEW`. Now this produces `ERROR 1176 (HY000): Key '...' doesn't exist in table '...'`, the same error as for base tables without an appropriate index. (Bug #33461)
- Cached queries that used 256 or more tables were not properly cached, so that later query invalidation due to a `TRUNCATE TABLE` for one of the tables caused the server to hang. (Bug #33362)
- Some division operations produced a result with incorrect precision. (Bug #31616)
- `mysql_upgrade` attempted to use the `/proc` file system even on systems that do not have it. (Bug #31605)
- `mysqldump` could fail to dump views containing a large number of columns. (Bug #31434)
- Queries executed using join buffering of `BIT` columns could produce incorrect results. (Bug #31399)
- `ALTER TABLE CONVERT TO CHARACTER SET` did not convert `TINYTEXT` or `MEDIUMTEXT` columns to a longer text type if necessary when converting the column to a different character set. (Bug #31291)
- For installation on Solaris using `pkgadd` packages, the `mysql_install_db` script was generated in the `scripts` directory, but the temporary files used during the process were left there and not deleted. (Bug #31052)

- Several MySQL programs could fail if the `HOME` environment variable had an empty value. (Bug #30394)
- On NetWare, `mysql_install_db` could appear to execute normally even if it failed to create the initial databases. (Bug #30129)
- The Serbian translation for the `ER_INCORRECT_GLOBAL_LOCAL_VAR` error was corrected. (Bug #29738)
- XA transaction rollbacks could result in corrupted transaction states and a server crash. (Bug #28323)
- The `BUILD/check-cpu` build script failed if `gcc` had a different name (such as `gcc.real` on Debian). (Bug #27526)
- On Windows, Visual Studio does not take into account some x86 hardware limitations, which led to incorrect results converting large `DOUBLE` values to unsigned `BIGINT` values. (Bug #27483)
- SSL support was not included in some “generic” RPM packages. (Bug #26760)
- In some cases, the parser interpreted the `;` character as the end of input and misinterpreted stored program definitions. (Bug #26030)
- The `Questions` status variable is intended as a count of statements sent by clients to the server, but was also counting statements executed within stored routines. (Bug #24289)
- For access to the `INFORMATION_SCHEMA.VIEWS` table, the server did not check the `SHOW VIEW` and `SELECT` privileges, leading to inconsistency between output from that table and the `SHOW CREATE VIEW` statement. (Bug #22763)
- The `FLUSH PRIVILEGES` statement did not produce an error when it failed. (Bug #21226)
- A race condition between the `mysqld.exe` server and the Windows service manager could lead to inability to stop the server from the service manager. (Bug #20430)
- `mysqld_safe` would sometimes fail to remove the pid file for the old `mysql` process after a crash. As a result, the server failed to start due to a false `A mysqld process already exists...` error. (Bug #11122)

Changes in MySQL Enterprise 5.0.76 [MRU] (2009-01-05)

This is a *Monthly Rapid Update* release of the MySQL Enterprise Server 5.0.

This section documents all changes and bugfixes that have been applied since the last MySQL Enterprise Server release (5.0.74). If you would like to receive more fine-grained and personalized *update alerts* about fixes that are relevant to the version and features you use, please consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details please see <http://www.mysql.com/products/enterprise/advisors.html>.

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- A new status variable, `Queries`, indicates the number of statements executed by the server. This includes statements executed within stored programs, unlike the `Questions` variable which includes only statements sent to the server by clients. (Bug #41131)

Bugs Fixed

- **Replication:** When rotating relay log files, the slave deletes relay log files and then edits the relay log index file. Formerly, if the slave shut down unexpectedly between these two events, the relay log index file could then reference relay logs that no longer existed. Depending on the circumstances, this could when restarting the slave cause either a race condition or the failure of replication. (Bug #38826, Bug #39325)
- In example option files provided in MySQL distributions, the `thread_stack` value was increased from 64K to 128K. (Bug #41577)
- `SET PASSWORD` caused a server crash if the account name was given as `CURRENT_USER()`. (Bug #41456)
- The `INFORMATION_SCHEMA.SCHEMA_PRIVILEGES` table was limited to 7680 rows. (Bug #41079)
- In debug builds, obsolete debug code could be used to crash the server. (Bug #41041)
- Some queries that used a “range checked for each record” scan could return incorrect results. (Bug #40974)

References: See also: Bug #44810.

- Certain `SELECT` queries could fail with a `Duplicate entry` error. (Bug #40953)
- `IF(..., CAST(longtext_val AS UNSIGNED), signed_val)` as an argument to an aggregate function could cause an assertion failure. (Bug #40761)
- The server crashed if an integer field in a CSV file did not have delimiting quotation marks. (Bug #39616)
- Creating a table with a comment of 62 characters or longer caused a server crash. (Bug #39591)
- `InnoDB` could hang trying to open an adaptive hash index. (Bug #39483)
- Use of spatial data types in prepared statements could cause memory leaks or server crashes. (Bug #37956, Bug #37671)
- The `MONTHNAME()` and `DAYNAME()` functions returned a binary string, so that using `LOWER()` or `UPPER()` had no effect. Now `MONTHNAME()` and `DAYNAME()` return a value in `character_set_connection` character set. (Bug #37575)
- Certain boolean-mode `FULLTEXT` searches that used the truncation operator did not return matching records and calculated relevance incorrectly. (Bug #37245)
- The code for the `ut_usec_time()` function in `InnoDB` did not handle errors from the `gettimeofday()` system call. Now it retries `gettimeofday()` several times and updates the value of the `InnoDB_row_lock_time_max` status variable only if `ut_usec_time()` was successful. (Bug #36819)
- A read past the end of the string could occur while parsing the value of the `--innodb-data-file-path` option. (Bug #36149)
- `SHOW CREATE TABLE` did not display a printable value for the default value of `BIT` columns. (Bug #35796)
- The `max_length` metadata value was calculated incorrectly for the `FORMAT()` function, which could cause incorrect result set metadata to be sent to clients. (Bug #35558)
- `EXPLAIN EXTENDED` evaluation of aggregate functions that required a temporary table caused a server crash. (Bug #34773)
- The `mysql` client incorrectly parsed statements containing the word “delimiter” in mid-statement.

This fix is different from the one applied for this bug in MySQL 5.0.66. (Bug #33812)

References: See also: Bug #38158.

- Queries executed using join buffering of `BIT` columns could produce incorrect results. (Bug #31399)
- `ALTER TABLE CONVERT TO CHARACTER SET` did not convert `TINYTEXT` or `MEDIUMTEXT` columns to a longer text type if necessary when converting the column to a different character set. (Bug #31291)
- On Windows, Visual Studio does not take into account some x86 hardware limitations, which led to incorrect results converting large `DOUBLE` values to unsigned `BIGINT` values. (Bug #27483)
- SSL support was not included in some “generic” RPM packages. (Bug #26760)

Changes in MySQL Community Server 5.0.75 (2008-12-17)

This is a bugfix release for the current MySQL Community Server production release family. It replaces MySQL 5.0.67.

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- **Security Enhancement:** To enable stricter control over the location from which user-defined functions can be loaded, the `plugin_dir` system variable has been backported from MySQL 5.1. If the value is nonempty, user-defined function object files can be loaded only from the directory named by this variable. If the value is empty, the behavior that is used prior to the inclusion of `plugin_dir` applies: The UDF object files must be located in a directory that is searched by your system's dynamic linker.

If the plugin directory is writable by the server, it may be possible for a user to write executable code to a file in the directory using `SELECT ... INTO DUMPFILE`. This can be prevented by making `plugin_dir` read only to the server or by setting `--secure-file-priv` to a directory where `SELECT` writes can be made safely. (Bug #37428)

- Previously, index hints did not work for `FULLTEXT` searches. Now they work as follows:

For natural language mode searches, index hints are silently ignored. For example, `IGNORE INDEX(i)` is ignored with no warning and the index is still used.

For boolean mode searches, index hints are honored. (Bug #38842)

Bugs Fixed

- **Security Fix; Important Change:** Additional corrections were made for the symlink-related privilege problem originally addressed in MySQL 5.0.60. The original fix did not correctly handle the data directory path name if it contained symlinked directories in its path, and the check was made only at table-creation time, not at table-opening time later. (Bug #32167, CVE-2008-2079)

References: See also: Bug #39277.

- **Security Enhancement:** The server consumed excess memory while parsing statements with hundreds or thousands of nested boolean conditions (such as `OR (OR ... (OR ...))`). This could lead to a server crash or incorrect statement execution, or cause other client statements to fail due to lack of memory. The latter result constitutes a denial of service. (Bug #38296)

- **Incompatible Change:** There were some problems using `DllMain()` hook functions on Windows that automatically do global and per-thread initialization for `libmysqld.dll`:
 - Per-thread initialization: MySQL internally counts the number of active threads, which causes a delay in `my_end()` if not all threads have exited. But there are threads that can be started either by Windows internally (often in TCP/IP scenarios) or by users. Those threads do not necessarily use `libmysql.dll` functionality but still contribute to the open-thread count. (One symptom is a five-second delay in times for PHP scripts to finish.)
 - Process-initialization: `my_init()` calls `WSAStartup` that itself loads DLLs and can lead to a deadlock in the Windows loader.

To correct these problems, DLL initialization code now is not invoked from `libmysql.dll` by default. To obtain the previous behavior (DLL initialization code will be called), set the `LIBMYSQL_DLLINIT` environment variable to any value. This variable exists only to prevent breakage of existing Windows-only applications that do not call `mysql_thread_init()` and work okay today. Use of `LIBMYSQL_DLLINIT` is discouraged and is removed in MySQL 6.0. (Bug #37226, Bug #33031)

- **Incompatible Change:** `SHOW STATUS` took a lot of CPU time for calculating the value of the `InnoDB_buffer_pool_pages_latched` status variable. Now this variable is calculated and included in the output of `SHOW STATUS` only if the `UNIV_DEBUG` symbol is defined at MySQL build time. (Bug #36600)
- **Incompatible Change:** In connection with view creation, the server created `arc` directories inside database directories and maintained useless copies of `.frm` files there. Creation and renaming procedures of those copies as well as creation of `arc` directories has been discontinued.

This change does cause a problem when downgrading to older server versions which manifests itself under these circumstances:

1. Create a view `v_orig` in MySQL 5.0.72 or higher.
2. Rename the view to `v_new` and then back to `v_orig`.
3. Downgrade to an older 5.0.x server and run `mysql_upgrade`.
4. Try to rename `v_orig` to `v_new` again. This operation fails.

As a workaround to avoid this problem, use either of these approaches:

- Dump your data using `mysqldump` before downgrading and reload the dump file after downgrading.
- Instead of renaming a view after the downgrade, drop it and recreate it.

The downgrade problem introduced by the fix for this bug has been addressed as Bug #40021. (Bug #17823)

References: See also: Bug #40021.

- `CHECK TABLE ... FOR UPGRADE` did not check for incompatible collation changes made in MySQL 5.0.48 (Bug #27562, Bug #29461, Bug #29499). This also affects `mysqlcheck` and `mysql_upgrade`, which cause that statement to be executed. See [Checking Whether Tables or Indexes Must Be Rebuilt](#). (Bug #40984)

References: See also: Bug #39585, Bug #27562, Bug #29461, Bug #29499.

- The `FEDERATED` handler had a memory leak. (Bug #40875)

- Prepared statements permitted invalid dates to be inserted when the [ALLOW_INVALID_DATES](#) SQL mode was not enabled. (Bug #40365)
- `mc.exe` is no longer needed to compile MySQL on Windows. This makes it possible to build MySQL from source using Visual Studio Express 2008. (Bug #40280)
- Support for the `revision` field in `.frm` files has been removed. This addresses the downgrading problem introduced by the fix for Bug #17823. (Bug #40021)

References: See also: Bug #17823.

- If the operating system is configured to return leap seconds from OS time calls or if the MySQL server uses a time zone definition that has leap seconds, functions such as `NOW()` could return a value having a time part that ends with `:59:60` or `:59:61`. If such values are inserted into a table, they would be dumped as is by `mysqldump` but considered invalid when reloaded, leading to backup/restore problems.

Now leap second values are returned with a time part that ends with `:59:59`. This means that a function such as `NOW()` can return the same value for two or three consecutive seconds during the leap second. It remains true that literal temporal values having a time part that ends with `:59:60` or `:59:61` are considered invalid.

For additional details about leap-second handling, see [Time Zone Leap Second Support](#). (Bug #39920)

- The server could crash during a sort-order optimization of a dependent subquery. (Bug #39844)
- With the [ONLY_FULL_GROUP_BY](#) SQL mode enabled, the check for nonaggregated columns in queries with aggregate functions, but without a `GROUP BY` clause was treating all the parts of the query as if they were in the select list. This is fixed by ignoring the nonaggregated columns in the `WHERE` clause. (Bug #39656)
- `CHECK TABLE` failed for `MyISAM INFORMATION_SCHEMA` tables. (Bug #39541)
- For a `TIMESTAMP` column in an `InnoDB` table, testing the column with multiple conditions in the `WHERE` clause caused a server crash. (Bug #39353)
- The server returned a column type of `VARBINARY` rather than `DATE` as the result from the `COALESCE()`, `IFNULL()`, `IF()`, `GREATEST()`, or `LEAST()` functions or `CASE` expression if the result was obtained using `filesort` in an anonymous temporary table during the query execution. (Bug #39283)
- References to local variables in stored procedures are replaced with `NAME_CONST(name, value)` when written to the binary log. However, an “illegal mix of collation” error might occur when executing the log contents if the value's collation differed from that of the variable. Now information about the variable collation is written as well. (Bug #39182)
- Some recent releases for Solaris 10 were built on Solaris 10 U5, which included a new version of `libnsl.so` that does not work on U4 or earlier. To correct this, Solaris 10 builds now are created on machines that do not have that upgraded `libnsl.so`, so that they will work on Solaris 10 installations both with and without the upgraded `libnsl.so`. (Bug #39074)
- With binary logging enabled `CREATE VIEW` was subject to possible buffer overwrite and a server crash. (Bug #39040)
- Queries of the form `SELECT ... REGEXP BINARY NULL` could lead to a hung or crashed server. (Bug #39021)
- Statements of the form `INSERT ... SELECT .. ON DUPLICATE KEY UPDATE col_name = DEFAULT` could result in a server crash. (Bug #39002)

- Column names constructed due to wild-card expansion done inside a stored procedure could point to freed memory if the expansion was performed after the first call to the stored procedure. (Bug #38823)
- Repeated `CREATE TABLE ... SELECT` statements, where the created table contained an `AUTO_INCREMENT` column, could lead to an assertion failure. (Bug #38821)
- If delayed insert failed to upgrade the lock, it did not free the temporary memory storage used to keep newly constructed `BLOB` values in memory, resulting in a memory leak. (Bug #38693)
- A server crash resulted from concurrent execution of a multiple-table `UPDATE` that used a `NATURAL` or `USING` join together with `FLUSH TABLES WITH READ LOCK` or `ALTER TABLE` for the table being updated. (Bug #38691)
- On ActiveState Perl, `mysql-test-run.pl --start-and-exit` started but did not exit. (Bug #38629)
- Server-side cursors were not initialized properly, which could cause a server crash. (Bug #38486)
- Stored procedures involving substrings could crash the server on certain platforms due to invalid memory reads. (Bug #38469)
- A server crash or Valgrind warnings could result when a stored procedure selected from a view that referenced a function. (Bug #38291)
- Incorrect handling of aggregate functions when loose index scan was used caused a server crash. (Bug #38195)
- Queries containing a subquery with `DISTINCT` and `ORDER BY` could cause a server crash. (Bug #38191)
- Queries with a `HAVING` clause could return a spurious row. (Bug #38072)
- The server crashed if an argument to a stored procedure was a subquery that returned more than one row. (Bug #37949)
- When analyzing the possible index use cases, the server was incorrectly reusing an internal structure, leading to a server crash. (Bug #37943)
- A `SELECT` with a `NULL NOT IN` condition containing a complex subquery from the same table as in the outer select caused an assertion failure. (Bug #37894)
- For `InnoDB` tables, `ORDER BY ... DESC` sometimes returned results in ascending order. (Bug #37830)
- If a table has a `BIT NOT NULL` column `c1` with a length shorter than 8 bits and some additional `NOT NULL` columns `c2`, ..., and a `SELECT` query has a `WHERE` clause of the form `(c1 = constant) AND c2 ...`, the query could return an unexpected result set. (Bug #37799)
- Nesting of `IF()` inside of `SUM()` could cause an extreme server slowdown. (Bug #37662)
- `TIMEDIFF()` was erroneously treated as always returning a positive result. Also, `CAST()` of `TIME` values to `DECIMAL` dropped the sign of negative values. (Bug #37553)

References: See also: Bug #42525.

- `mysqlcheck` used `SHOW FULL TABLES` to get the list of tables in a database. For some problems, such as an empty `.frm` file for a table, this failed and `mysqlcheck` then would neglect to check other tables in the database. (Bug #37527)

- The `<=>` operator could return incorrect results when comparing `NULL` to `DATE`, `TIME`, or `DATETIME` values. (Bug #37526)
- Updating a view with a subquery in the `CHECK` option could cause an assertion failure. (Bug #37460)
- Statements that displayed the value of system variables (for example, `SHOW VARIABLES`) expect variable values to be encoded in `character_set_system`. However, variables set from the command line such as `basedir` or `datadir` were encoded using `character_set_filesystem` and not converted correctly. (Bug #37339)
- For a `MyISAM` table with `CHECKSUM = 1` and `ROW_FORMAT = DYNAMIC` table options, a data consistency check (maximum record length) could fail and cause the table to be marked as corrupted. (Bug #37310)
- The `max_length` result set metadata value was calculated incorrectly under some circumstances. (Bug #37301)
- `CREATE INDEX` could crash with `InnoDB` plugin 1.0.1. (Bug #37284)
- The `NO_BACKSLASH_ESCAPES` SQL mode was ignored for `LOAD DATA INFILE` and `SELECT INTO ... OUTFILE`. The setting is taken into account now. (Bug #37114)
- On a 32-bit server built without big tables support, the offset argument in a `LIMIT` clause might be truncated due to a 64-bit to 32-bit cast. (Bug #37075)
- If the server failed to expire binary log files at startup, it could crash. (Bug #37027)
- Use of `CONVERT()` with `GROUP BY` to convert numeric values to `CHAR` could return truncated results. (Bug #36772)
- A query which had an `ORDER BY DESC` clause that is satisfied with a reverse range scan could cause a server crash for some specific CPU/compiler combinations. (Bug #36639)
- Dumping information about locks in use by sending a `SIGHUP` signal to the server or by invoking the `mysqladmin debug` command could lead to a server crash in debug builds or to undefined behavior in production builds. (Bug #36579)
- The `mysql` client, when built with Visual Studio 2005, did not display Japanese characters. (Bug #36279)
- When the fractional part in a multiplication of `DECIMAL` values overflowed, the server truncated the first operand rather than the longest. Now the server truncates so as to produce more precise multiplications. (Bug #36270)
- Host name values in SQL statements were not being checked for `'@'`, which is illegal according to RFC952. (Bug #35924)
- The `UUID()` function returned UUIDs with the wrong time; this was because the offset for the time part in UUIDs was miscalculated. (Bug #35848)
- `mysql_install_db` failed on machines that had the host name set to `localhost`. (Bug #35754)
- Dynamic plugins failed to load on i5/OS. (Bug #35743)
- Freeing of an internal parser stack during parsing of complex stored programs caused a server crash. (Bug #35577, Bug #37269, Bug #37228)
- Index scans performed with the `sort_union()` access method returned wrong results, caused memory to be leaked, and caused temporary files to be deleted when the limit set by `sort_buffer_size` was reached. (Bug #35477, Bug #35478)

- If the server crashed with an `InnoDB` error due to unavailability of undo slots, errors could persist during rollback when the server was restarted: There are two `UNDO` slot caches (for `INSERT` and `UPDATE`). If all slots end up in one of the slot caches, a request for a slot from the other slot cache failed. This can happen if the request is for an `UPDATE` slot and all slots are in the `INSERT` slot cache, or vice versa. (Bug #35352)
- For `InnoDB` tables, `ALTER TABLE DROP` failed if the name of the column to be dropped began with "foreign". (Bug #35220)
- `perror` on Windows did not know about Win32 system error codes. (Bug #34825)
- Queries of the form `SELECT ... WHERE string = ANY(...)` failed when the server used a single-byte character set and the client used a multibyte character set. (Bug #34760)

References: See also: Bug #20835.

- Using `OPTIMIZE TABLE` as the first statement on an `InnoDB` table with an `AUTO_INCREMENT` column could cause a server crash. (Bug #34286)
- `mysql_install_db` failed if the server was running with an SQL mode of `TRADITIONAL`. This program now resets the SQL mode internally to avoid this problem. (Bug #34159)
- Changes to build files were made to enable the MySQL distribution to compile on Microsoft Visual C++ Express 2008. (Bug #33907)
- For a stored procedure containing a `SELECT * ... RIGHT JOIN` query, execution failed for the second call. (Bug #33811)
- Previously, use of index hints with views (which do not have indexes) produced the error `ERROR 1221 (HY000): Incorrect usage of USE/IGNORE INDEX and VIEW`. Now this produces `ERROR 1176 (HY000): Key '...' doesn't exist in table '...'`, the same error as for base tables without an appropriate index. (Bug #33461)
- Cached queries that used 256 or more tables were not properly cached, so that later query invalidation due to a `TRUNCATE TABLE` for one of the tables caused the server to hang. (Bug #33362)
- Some division operations produced a result with incorrect precision. (Bug #31616)
- `mysql_upgrade` attempted to use the `/proc` file system even on systems that do not have it. (Bug #31605)
- `mysqldump` could fail to dump views containing a large number of columns. (Bug #31434)
- Several MySQL programs could fail if the `HOME` environment variable had an empty value. (Bug #30394)
- On NetWare, `mysql_install_db` could appear to execute normally even if it failed to create the initial databases. (Bug #30129)
- The Serbian translation for the `ER_INCORRECT_GLOBAL_LOCAL_VAR` error was corrected. (Bug #29738)
- XA transaction rollbacks could result in corrupted transaction states and a server crash. (Bug #28323)
- The `BUILD/check-cpu` build script failed if `gcc` had a different name (such as `gcc.real` on Debian). (Bug #27526)
- In some cases, the parser interpreted the `;` character as the end of input and misinterpreted stored program definitions. (Bug #26030)

- The `Questions` status variable is intended as a count of statements sent by clients to the server, but was also counting statements executed within stored routines. (Bug #24289)
- For access to the `INFORMATION_SCHEMA.VIEWS` table, the server did not check the `SHOW VIEW` and `SELECT` privileges, leading to inconsistency between output from that table and the `SHOW CREATE VIEW` statement. (Bug #22763)
- The `FLUSH PRIVILEGES` statement did not produce an error when it failed. (Bug #21226)
- A race condition between the `mysqld.exe` server and the Windows service manager could lead to inability to stop the server from the service manager. (Bug #20430)
- `mysqld_safe` would sometimes fail to remove the pid file for the old `mysql` process after a crash. As a result, the server failed to start due to a false `A mysqld process already exists...` error. (Bug #11122)

Changes in MySQL Enterprise 5.0.74sp1 [QSP] (2009-04-30)

This is a *Service Pack* release of the MySQL Enterprise Server 5.0.

This section documents all changes and bugfixes that have been applied since the last MySQL Enterprise Server release (5.0.74).

If you would like to receive more fine-grained and personalized *update alerts* about fixes that are relevant to the version and features you use, please consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details please see <http://www.mysql.com/products/enterprise/advisors.html>.

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- The `libedit` library was upgraded to version 2.11. (Bug #42433)

Bugs Fixed

- An attempt by a user who did not have the `SUPER` privilege to kill a system thread could cause a server crash. (Bug #43748)
- Tables could enter open table cache for a thread without being properly cleaned up, leading to a server crash. (Bug #42419)
- The SSL certificates included with MySQL distributions were regenerated because the previous ones had expired. (Bug #42366)
- Some queries using `NAME_CONST(... COLLATE ...)` led to a server crash due to a failed type cast. (Bug #42014)
- `DATE_FORMAT()` could cause a server crash for year-zero dates. (Bug #41470)
- `SET PASSWORD` caused a server crash if the account name was given as `CURRENT_USER()`. (Bug #41456)
- When substituting system constant functions with a constant result, the server was not expecting `NULL` function return values and could crash. (Bug #41437)
- Creating a table with a comment of 62 characters or longer caused a server crash. (Bug #39591)

- [EXPLAIN EXTENDED](#) evaluation of aggregate functions that required a temporary table caused a server crash. (Bug #34773)

Changes in MySQL Enterprise 5.0.74 [MRU] (2008-12-03)

This is a *Monthly Rapid Update* release of the MySQL Enterprise Server 5.0.

This section documents all changes and bugfixes that have been applied since the last MySQL Enterprise Server release (5.0.72). If you would like to receive more fine-grained and personalized *update alerts* about fixes that are relevant to the version and features you use, please consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details please see <http://www.mysql.com/products/enterprise/advisors.html>.

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- Previously, index hints did not work for [FULLTEXT](#) searches. Now they work as follows:

For natural language mode searches, index hints are silently ignored. For example, `IGNORE INDEX(i)` is ignored with no warning and the index is still used.

For boolean mode searches, index hints are honored. (Bug #38842)

Bugs Fixed

- [CHECK TABLE ... FOR UPGRADE](#) did not check for incompatible collation changes made in MySQL 5.0.48 (Bug #27562, Bug #29461, Bug #29499). This also affects `mysqlcheck` and `mysql_upgrade`, which cause that statement to be executed. See [Checking Whether Tables or Indexes Must Be Rebuilt](#). (Bug #40984)

References: See also: Bug #39585, Bug #27562, Bug #29461, Bug #29499.

- The [FEDERATED](#) handler had a memory leak. (Bug #40875)
- Prepared statements permitted invalid dates to be inserted when the [ALLOW_INVALID_DATES](#) SQL mode was not enabled. (Bug #40365)
- Support for the `revision` field in `.frm` files has been removed. This addresses the downgrading problem introduced by the fix for Bug #17823. (Bug #40021)

References: See also: Bug #17823.

- If the operating system is configured to return leap seconds from OS time calls or if the MySQL server uses a time zone definition that has leap seconds, functions such as `NOW()` could return a value having a time part that ends with `:59:60` or `:59:61`. If such values are inserted into a table, they would be dumped as is by `mysqldump` but considered invalid when reloaded, leading to backup/restore problems.

Now leap second values are returned with a time part that ends with `:59:59`. This means that a function such as `NOW()` can return the same value for two or three consecutive seconds during the leap second. It remains true that literal temporal values having a time part that ends with `:59:60` or `:59:61` are considered invalid.

For additional details about leap-second handling, see [Time Zone Leap Second Support](#). (Bug #39920)

- With the `ONLY_FULL_GROUP_BY` SQL mode enabled, the check for nonaggregated columns in queries with aggregate functions, but without a `GROUP BY` clause was treating all the parts of the query as if they were in the select list. This is fixed by ignoring the nonaggregated columns in the `WHERE` clause. (Bug #39656)
- `CHECK TABLE` failed for `MyISAM INFORMATION_SCHEMA` tables. (Bug #39541)
- With binary logging enabled `CREATE VIEW` was subject to possible buffer overwrite and a server crash. (Bug #39040)
- Queries with a `HAVING` clause could return a spurious row. (Bug #38072)
- `TIMEDIFF()` was erroneously treated as always returning a positive result. Also, `CAST()` of `TIME` values to `DECIMAL` dropped the sign of negative values. (Bug #37553)

References: See also: Bug #42525.

- `mysqlcheck` used `SHOW FULL TABLES` to get the list of tables in a database. For some problems, such as an empty `.frm` file for a table, this failed and `mysqlcheck` then would neglect to check other tables in the database. (Bug #37527)
- Updating a view with a subquery in the `CHECK` option could cause an assertion failure. (Bug #37460)
- Statements that displayed the value of system variables (for example, `SHOW VARIABLES`) expect variable values to be encoded in `character_set_system`. However, variables set from the command line such as `basedir` or `datadir` were encoded using `character_set_filesystem` and not converted correctly. (Bug #37339)
- `CREATE INDEX` could crash with `InnoDB` plugin 1.0.1. (Bug #37284)
- Use of `CONVERT()` with `GROUP BY` to convert numeric values to `CHAR` could return truncated results. (Bug #36772)
- The `mysql` client, when built with Visual Studio 2005, did not display Japanese characters. (Bug #36279)
- `perror` on Windows did not know about Win32 system error codes. (Bug #34825)
- Queries of the form `SELECT ... WHERE string = ANY(...)` failed when the server used a single-byte character set and the client used a multibyte character set. (Bug #34760)

References: See also: Bug #20835.

- For a stored procedure containing a `SELECT * ... RIGHT JOIN` query, execution failed for the second call. (Bug #33811)
- Previously, use of index hints with views (which do not have indexes) produced the error `ERROR 1221 (HY000): Incorrect usage of USE/IGNORE INDEX and VIEW`. Now this produces `ERROR 1176 (HY000): Key '...' doesn't exist in table '...'`, the same error as for base tables without an appropriate index. (Bug #33461)
- Some division operations produced a result with incorrect precision. (Bug #31616)
- A race condition between the `mysqld.exe` server and the Windows service manager could lead to inability to stop the server from the service manager. (Bug #20430)

Changes in MySQL Enterprise 5.0.72sp1 [QSP] (2009-01-13)

This is a *Service Pack* release of the MySQL Enterprise Server 5.0.

This section documents all changes and bugfixes that have been applied since the last MySQL Enterprise Server release (5.0.72).

If you would like to receive more fine-grained and personalized *update alerts* about fixes that are relevant to the version and features you use, please consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details please see <http://www.mysql.com/products/enterprise/advisors.html>.

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- Previously, index hints did not work for `FULLTEXT` searches. Now they work as follows:

For natural language mode searches, index hints are silently ignored. For example, `IGNORE INDEX(i)` is ignored with no warning and the index is still used.

For boolean mode searches, index hints are honored. (Bug #38842)

Bugs Fixed

- **MySQL Cluster; Packaging:** Packages for MySQL Cluster were missing the `libndbclient.so` and `libndbclient.a` files. (Bug #42278)

- Support for the `revision` field in `.frm` files has been removed. This addresses the downgrading problem introduced by the fix for Bug #17823. (Bug #40021)

References: See also: Bug #17823.

- If the operating system is configured to return leap seconds from OS time calls or if the MySQL server uses a time zone definition that has leap seconds, functions such as `NOW()` could return a value having a time part that ends with `:59:60` or `:59:61`. If such values are inserted into a table, they would be dumped as is by `mysqldump` but considered invalid when reloaded, leading to backup/restore problems.

Now leap second values are returned with a time part that ends with `:59:59`. This means that a function such as `NOW()` can return the same value for two or three consecutive seconds during the leap second. It remains true that literal temporal values having a time part that ends with `:59:60` or `:59:61` are considered invalid.

For additional details about leap-second handling, see [Time Zone Leap Second Support](#). (Bug #39920)

- Queries of the form `SELECT ... WHERE string = ANY(...)` failed when the server used a single-byte character set and the client used a multibyte character set. (Bug #34760)

References: See also: Bug #20835.

Changes in MySQL Enterprise 5.0.72 [MRU] (2008-10-24)

This is a *Monthly Rapid Update* release of the MySQL Enterprise Server 5.0.

This section documents all changes and bugfixes that have been applied since the last MySQL Enterprise Server release (5.0.70). If you would like to receive more fine-grained and personalized *update alerts* about fixes that are relevant to the version and features you use, please consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details please see <http://www.mysql.com/products/enterprise/advisors.html>.

Bugs Fixed

- **Incompatible Change:** In connection with view creation, the server created `arc` directories inside database directories and maintained useless copies of `.frm` files there. Creation and renaming procedures of those copies as well as creation of `arc` directories has been discontinued.

This change does cause a problem when downgrading to older server versions which manifests itself under these circumstances:

1. Create a view `v_orig` in MySQL 5.0.72 or higher.
2. Rename the view to `v_new` and then back to `v_orig`.
3. Downgrade to an older 5.0.x server and run `mysql_upgrade`.
4. Try to rename `v_orig` to `v_new` again. This operation fails.

As a workaround to avoid this problem, use either of these approaches:

- Dump your data using `mysqldump` before downgrading and reload the dump file after downgrading.
- Instead of renaming a view after the downgrade, drop it and recreate it.

The downgrade problem introduced by the fix for this bug has been addressed as Bug #40021. (Bug #17823)

References: See also: Bug #40021.

- `mc.exe` is no longer needed to compile MySQL on Windows. This makes it possible to build MySQL from source using Visual Studio Express 2008. (Bug #40280)
- The server could crash during a sort-order optimization of a dependent subquery. (Bug #39844)
- The server returned a column type of `VARBINARY` rather than `DATE` as the result from the `COALESCE()`, `IFNULL()`, `IF()`, `GREATEST()`, or `LEAST()` functions or `CASE` expression if the result was obtained using `filesort` in an anonymous temporary table during the query execution. (Bug #39283)
- References to local variables in stored procedures are replaced with `NAME_CONST(name, value)` when written to the binary log. However, an “illegal mix of collation” error might occur when executing the log contents if the value's collation differed from that of the variable. Now information about the variable collation is written as well. (Bug #39182)
- Some recent releases for Solaris 10 were built on Solaris 10 U5, which included a new version of `libnsl.so` that does not work on U4 or earlier. To correct this, Solaris 10 builds now are created on machines that do not have that upgraded `libnsl.so`, so that they will work on Solaris 10 installations both with and without the upgraded `libnsl.so`. (Bug #39074)
- Column names constructed due to wild-card expansion done inside a stored procedure could point to freed memory if the expansion was performed after the first call to the stored procedure. (Bug #38823)
- If delayed insert failed to upgrade the lock, it did not free the temporary memory storage used to keep newly constructed `BLOB` values in memory, resulting in a memory leak. (Bug #38693)
- A server crash resulted from concurrent execution of a multiple-table `UPDATE` that used a `NATURAL` or `USING` join together with `FLUSH TABLES WITH READ LOCK` or `ALTER TABLE` for the table being updated. (Bug #38691)
- On ActiveState Perl, `mysql-test-run.pl --start-and-exit` started but did not exit. (Bug #38629)

- Stored procedures involving substrings could crash the server on certain platforms due to invalid memory reads. (Bug #38469)
- The server crashed if an argument to a stored procedure was a subquery that returned more than one row. (Bug #37949)
- When analyzing the possible index use cases, the server was incorrectly reusing an internal structure, leading to a server crash. (Bug #37943)
- A `SELECT` with a `NULL NOT IN` condition containing a complex subquery from the same table as in the outer select caused an assertion failure. (Bug #37894)
- On a 32-bit server built without big tables support, the offset argument in a `LIMIT` clause might be truncated due to a 64-bit to 32-bit cast. (Bug #37075)
- Host name values in SQL statements were not being checked for '@', which is illegal according to RFC952. (Bug #35924)
- `mysql_install_db` failed on machines that had the host name set to `localhost`. (Bug #35754)
- Dynamic plugins failed to load on i5/OS. (Bug #35743)
- XA transaction rollbacks could result in corrupted transaction states and a server crash. (Bug #28323)
- The `Questions` status variable is intended as a count of statements sent by clients to the server, but was also counting statements executed within stored routines. (Bug #24289)
- For access to the `INFORMATION_SCHEMA.VIEWS` table, the server did not check the `SHOW VIEW` and `SELECT` privileges, leading to inconsistency between output from that table and the `SHOW CREATE VIEW` statement. (Bug #22763)
- `mysqld_safe` would sometimes fail to remove the pid file for the old `mysql` process after a crash. As a result, the server failed to start due to a false `A mysqld process already exists...` error. (Bug #11122)

Changes in MySQL Enterprise 5.0.70 [MRU] (2008-09-27)

This is a *Monthly Rapid Update* release of the MySQL Enterprise Server 5.0.

This section documents all changes and bugfixes that have been applied since the last MySQL Enterprise Server release (5.0.68). If you would like to receive more fine-grained and personalized *update alerts* about fixes that are relevant to the version and features you use, please consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details please see <http://www.mysql.com/products/enterprise/advisors.html>.

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- **Security Enhancement:** To enable stricter control over the location from which user-defined functions can be loaded, the `plugin_dir` system variable has been backported from MySQL 5.1. If the value is nonempty, user-defined function object files can be loaded only from the directory named by this variable. If the value is empty, the behavior that is used prior to the inclusion of `plugin_dir` applies: The UDF object files must be located in a directory that is searched by your system's dynamic linker.

If the plugin directory is writable by the server, it may be possible for a user to write executable code to a file in the directory using `SELECT ... INTO DUMPFILE`. This can be prevented by making

`plugin_dir` read only to the server or by setting `--secure-file-priv` to a directory where `SELECT` writes can be made safely. (Bug #37428)

Bugs Fixed

- **Security Fix; Important Change:** Additional corrections were made for the symlink-related privilege problem originally addressed in MySQL 5.0.60. The original fix did not correctly handle the data directory path name if it contained symlinked directories in its path, and the check was made only at table-creation time, not at table-opening time later. (Bug #32167, CVE-2008-2079)

References: See also: Bug #39277.

- **Incompatible Change:** There were some problems using `DllMain()` hook functions on Windows that automatically do global and per-thread initialization for `libmysqld.dll`:
 - Per-thread initialization: MySQL internally counts the number of active threads, which causes a delay in `my_end()` if not all threads have exited. But there are threads that can be started either by Windows internally (often in TCP/IP scenarios) or by users. Those threads do not necessarily use `libmysql.dll` functionality but still contribute to the open-thread count. (One symptom is a five-second delay in times for PHP scripts to finish.)
 - Process-initialization: `my_init()` calls `WSAStartup` that itself loads DLLs and can lead to a deadlock in the Windows loader.

To correct these problems, DLL initialization code now is not invoked from `libmysql.dll` by default. To obtain the previous behavior (DLL initialization code will be called), set the `LIBMYSQL_DLLINIT` environment variable to any value. This variable exists only to prevent breakage of existing Windows-only applications that do not call `mysql_thread_init()` and work okay today. Use of `LIBMYSQL_DLLINIT` is discouraged and is removed in MySQL 6.0. (Bug #37226, Bug #33031)

- For a `TIMESTAMP` column in an InnoDB table, testing the column with multiple conditions in the `WHERE` clause caused a server crash. (Bug #39353)
- Queries of the form `SELECT ... REGEXP BINARY NULL` could lead to a hung or crashed server. (Bug #39021)
- Statements of the form `INSERT ... SELECT .. ON DUPLICATE KEY UPDATE col_name = DEFAULT` could result in a server crash. (Bug #39002)
- Repeated `CREATE TABLE ... SELECT` statements, where the created table contained an `AUTO_INCREMENT` column, could lead to an assertion failure. (Bug #38821)
- A server crash or Valgrind warnings could result when a stored procedure selected from a view that referenced a function. (Bug #38291)
- Incorrect handling of aggregate functions when loose index scan was used caused a server crash. (Bug #38195)
- If a table has a `BIT NOT NULL` column `c1` with a length shorter than 8 bits and some additional `NOT NULL` columns `c2`, ..., and a `SELECT` query has a `WHERE` clause of the form `(c1 = constant) AND c2 ...`, the query could return an unexpected result set. (Bug #37799)
- The `<=>` operator could return incorrect results when comparing `NULL` to `DATE`, `TIME`, or `DATETIME` values. (Bug #37526)
- For a `MyISAM` table with `CHECKSUM = 1` and `ROW_FORMAT = DYNAMIC` table options, a data consistency check (maximum record length) could fail and cause the table to be marked as corrupted. (Bug #37310)

- The `max_length` result set metadata value was calculated incorrectly under some circumstances. (Bug #37301)
- The `NO_BACKSLASH_ESCAPES` SQL mode was ignored for `LOAD DATA INFILE` and `SELECT INTO ... OUTFILE`. The setting is taken into account now. (Bug #37114)
- A query which had an `ORDER BY DESC` clause that is satisfied with a reverse range scan could cause a server crash for some specific CPU/compiler combinations. (Bug #36639)
- Dumping information about locks in use by sending a `SIGHUP` signal to the server or by invoking the `mysqladmin debug` command could lead to a server crash in debug builds or to undefined behavior in production builds. (Bug #36579)
- When the fractional part in a multiplication of `DECIMAL` values overflowed, the server truncated the first operand rather than the longest. Now the server truncates so as to produce more precise multiplications. (Bug #36270)
- Changes to build files were made to enable the MySQL distribution to compile on Microsoft Visual C++ Express 2008. (Bug #33907)
- `mysqldump` could fail to dump views containing a large number of columns. (Bug #31434)
- Several MySQL programs could fail if the `HOME` environment variable had an empty value. (Bug #30394)
- The `BUILD/check-cpu` build script failed if `gcc` had a different name (such as `gcc.real` on Debian). (Bug #27526)

Changes in MySQL Enterprise 5.0.68 [MRU] (2008-08-13)

This is a *Monthly Rapid Update* release of the MySQL Enterprise Server 5.0.

This section documents all changes and bugfixes that have been applied since the last MySQL Enterprise Server release (5.0.66a). If you would like to receive more fine-grained and personalized *update alerts* about fixes that are relevant to the version and features you use, please consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details please see <http://www.mysql.com/products/enterprise/advisors.html>.

Bugs Fixed

- **Security Enhancement:** The server consumed excess memory while parsing statements with hundreds or thousands of nested boolean conditions (such as `OR (OR ... (OR ...))`). This could lead to a server crash or incorrect statement execution, or cause other client statements to fail due to lack of memory. The latter result constitutes a denial of service. (Bug #38296)
- **Incompatible Change:** `SHOW STATUS` took a lot of CPU time for calculating the value of the `InnoDB_buffer_pool_pages_latched` status variable. Now this variable is calculated and included in the output of `SHOW STATUS` only if the `UNIV_DEBUG` symbol is defined at MySQL build time. (Bug #36600)
- Server-side cursors were not initialized properly, which could cause a server crash. (Bug #38486)
- Queries containing a subquery with `DISTINCT` and `ORDER BY` could cause a server crash. (Bug #38191)
- For `InnoDB` tables, `ORDER BY ... DESC` sometimes returned results in ascending order. (Bug #37830)
- Nesting of `IF ()` inside of `SUM()` could cause an extreme server slowdown. (Bug #37662)

- If the server failed to expire binary log files at startup, it could crash. (Bug #37027)
- The `UUID()` function returned UUIDs with the wrong time; this was because the offset for the time part in UUIDs was miscalculated. (Bug #35848)
- Freeing of an internal parser stack during parsing of complex stored programs caused a server crash. (Bug #35577, Bug #37269, Bug #37228)
- Index scans performed with the `sort_union()` access method returned wrong results, caused memory to be leaked, and caused temporary files to be deleted when the limit set by `sort_buffer_size` was reached. (Bug #35477, Bug #35478)
- If the server crashed with an InnoDB error due to unavailability of undo slots, errors could persist during rollback when the server was restarted: There are two UNDO slot caches (for `INSERT` and `UPDATE`). If all slots end up in one of the slot caches, a request for a slot from the other slot cache failed. This can happen if the request is for an `UPDATE` slot and all slots are in the `INSERT` slot cache, or vice versa. (Bug #35352)
- For InnoDB tables, `ALTER TABLE DROP` failed if the name of the column to be dropped began with "foreign". (Bug #35220)
- Using `OPTIMIZE TABLE` as the first statement on an InnoDB table with an `AUTO_INCREMENT` column could cause a server crash. (Bug #34286)
- `mysql_install_db` failed if the server was running with an SQL mode of `TRADITIONAL`. This program now resets the SQL mode internally to avoid this problem. (Bug #34159)
- Cached queries that used 256 or more tables were not properly cached, so that later query invalidation due to a `TRUNCATE TABLE` for one of the tables caused the server to hang. (Bug #33362)
- `mysql_upgrade` attempted to use the `/proc` file system even on systems that do not have it. (Bug #31605)
- On NetWare, `mysql_install_db` could appear to execute normally even if it failed to create the initial databases. (Bug #30129)
- The Serbian translation for the `ER_INCORRECT_GLOBAL_LOCAL_VAR` error was corrected. (Bug #29738)
- In some cases, the parser interpreted the `;` character as the end of input and misinterpreted stored program definitions. (Bug #26030)
- The `FLUSH PRIVILEGES` statement did not produce an error when it failed. (Bug #21226)

Changes in MySQL Community Server 5.0.67 (2008-08-04)

This is a bugfix release for the current MySQL Community Server production release family. It replaces MySQL 5.0.51b.

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- **Security Enhancement:** To enable stricter control over the location from which user-defined functions can be loaded, the `plugin_dir` system variable has been backported from MySQL 5.1. If the value

is nonempty, user-defined function object files can be loaded only from the directory named by this variable. If the value is empty, the behavior that is used prior to the inclusion of `plugin_dir` applies: The UDF object files must be located in a directory that is searched by your system's dynamic linker.

If the plugin directory is writable by the server, it may be possible for a user to write executable code to a file in the directory using `SELECT ... INTO DUMPFILE`. This can be prevented by making `plugin_dir` read only to the server or by setting `--secure-file-priv` to a directory where `SELECT` writes can be made safely. (Bug #37428)

- **Incompatible Change; Important Change:** The `FEDERATED` storage engine is now disabled by default in the `.cnf` files shipped with MySQL distributions (`my-huge.cnf`, `my-medium.cnf`, and so forth). This affects server behavior only if you install one of these files. (Bug #37069)
- **Important Change; Cluster API:** Because `NDB_LE_MemoryUsage.page_size_kb` shows memory page sizes in bytes rather than kilobytes, it has been renamed to `page_size_bytes`. The name `page_size_kb` is now deprecated and thus subject to removal in a future release, although it currently remains supported for reasons of backward compatibility. See [The Ndb_logevent_type Type](#), for more information about `NDB_LE_MemoryUsage`. (Bug #30271)
- **Important Change:** Some changes were made to `CHECK TABLE ... FOR UPGRADE` and `REPAIR TABLE` with respect to detection and handling of tables with incompatible `.frm` files (files created with a different version of the MySQL server). These changes also affect `mysqlcheck` because that program uses `CHECK TABLE` and `REPAIR TABLE`, and thus also `mysql_upgrade` because that program invokes `mysqlcheck`.
 - If your table was created by a different version of the MySQL server than the one you are currently running, `CHECK TABLE ... FOR UPGRADE` indicates that the table has an `.frm` file with an incompatible version. In this case, the result set returned by `CHECK TABLE` contains a line with a `Msg_type` value of `error` and a `Msg_text` value of `Table upgrade required. Please do "REPAIR TABLE `tbl_name`" to fix it!`
 - `REPAIR TABLE` without `USE_FRM` upgrades the `.frm` file to the current version.
 - If you use `REPAIR TABLE ...USE_FRM` and your table was created by a different version of the MySQL server than the one you are currently running, `REPAIR TABLE` will not attempt to repair the table. In this case, the result set returned by `REPAIR TABLE` contains a line with a `Msg_type` value of `error` and a `Msg_text` value of `Failed repairing incompatible .FRM file.`

Previously, use of `REPAIR TABLE ...USE_FRM` with a table created by a different version of the MySQL server risked the loss of all rows in the table.

(Bug #36055)

- `mysql_upgrade` now has a `--tmpdir` option to enable the location of temporary files to be specified. (Bug #36469)
- `mysql-test-run.pl` now supports `--client-bindir` and `--client-libdir` options for specifying the directory where client binaries and libraries are located. (Bug #34995)
- The `ndbd` and `ndb_mgmd` man pages have been reclassified from volume 1 to volume 8. (Bug #34642)
- For binary `.tar.gz` packages, `mysqld` and other binaries now are compiled with debugging symbols included to enable easier use with a debugger. If you do not need debugging symbols and are short on disk space, you can use `strip` to remove the symbols from the binaries. (Bug #33252)
- `mysqldump` produces a `-- Dump completed on DATE` comment at the end of the dump if `--comments` is given. The date causes dump files for identical data take at different times to appear to be

different. The new options `--dump-date` and `--skip-dump-date` control whether the date is added to the comment. `--skip-dump-date` suppresses date printing. The default is `--dump-date` (include the date in the comment). (Bug #31077)

- `mysqltest` now has `mkdir` and `rmdir` commands for creating and removing directories. (Bug #31004)
- The `mysql_odbc_escape_string()` C API function has been removed. It has multibyte character escaping issues, doesn't honor the `NO_BACKSLASH_ESCAPES` SQL mode and is not needed anymore by Connector/ODBC as of 3.51.17. (Bug #29592)

References: See also: Bug #41728.

- The default value of the `connect_timeout` system variable was increased from 5 to 10 seconds. This might help in cases where clients frequently encounter errors of the form `Lost connection to MySQL server at 'XXX', system error: errno`. (Bug #28359)
- The use of InnoDB hash indexes now can be controlled by setting the new `innodb_adaptive_hash_index` system variable at server startup. By default, this variable is enabled. See [Adaptive Hash Indexes](#).
- The argument for the `mysql-test-run.pl --do-test` and `--skip-test` options is now interpreted as a Perl regular expression if there is a pattern metacharacter in the argument value. This enables more flexible specification of which tests to perform or skip.

Bugs Fixed

- **Security Fix; Important Change:** It was possible to circumvent privileges through the creation of `MyISAM` tables employing the `DATA DIRECTORY` and `INDEX DIRECTORY` options to overwrite existing table files in the MySQL data directory. Use of the MySQL data directory in `DATA DIRECTORY` and `INDEX DIRECTORY` path name is no longer permitted.



Note

Additional fixes were made in MySQL 5.0.70.

(Bug #32167, CVE-2008-2079)

References: See also: Bug #39277.

- **Security Fix:** Three vulnerabilities in yaSSL versions 1.7.5 and earlier were discovered that could lead to a server crash or execution of unauthorized code. The exploit requires a server with yaSSL enabled and TCP/IP connections enabled, but does not require valid MySQL account credentials. The exploit does not apply to OpenSSL.



Warning

The proof-of-concept exploit is freely available on the Internet. Everyone with a vulnerable MySQL configuration is advised to upgrade *immediately*.

(Bug #33814, CVE-2008-0226, CVE-2008-0227)

- **Security Fix:** Using `RENAME TABLE` against a table with explicit `DATA DIRECTORY` and `INDEX DIRECTORY` options can be used to overwrite system table information by replacing the symbolic link points. the file to which the symlink points.

MySQL will now return an error when the file to which the symlink points already exists. (Bug #32111, CVE-2007-5969)

- **Security Fix:** `ALTER VIEW` retained the original `DEFINER` value, even when altered by another user, which could enable that user to gain the access rights of the view. Now `ALTER VIEW` is permitted only to the original definer or users with the `SUPER` privilege. (Bug #29908)
- **Security Fix:** When using a `FEDERATED` table, the local server could be forced to crash if the remote server returned a result with fewer columns than expected. (Bug #29801)
- **Security Enhancement:** It was possible to force an error message of excessive length which could lead to a buffer overflow. This has been made no longer possible as a security precaution. (Bug #32707)
- **Performance:** `InnoDB` adaptive hash latches could be held too long during filesort operations, resulting in a server crash. Now the hash latch is released when a query on `InnoDB` tables performs a filesort. This eliminates the crash and may provide significant performance improvements on systems on which many queries using filesorts with temporary tables are being performed. (Bug #32149)
- **Performance:** `InnoDB` had a race condition for an adaptive hash rw-lock waiting for an X-lock. This fix may also provide significant speed improvements on systems experiencing problems with contention for the adaptive hash index. (Bug #29560)
- **Incompatible Change:** It was possible to use `FRAC_SECOND` as a synonym for `MICROSECOND` with `DATE_ADD()`, `DATE_SUB()`, and `INTERVAL`; now, using `FRAC_SECOND` with anything other than `TIMESTAMPADD()` or `TIMESTAMPDIFF()` produces a syntax error.

It is now possible (and preferable) to use `MICROSECOND` with `TIMESTAMPADD()` and `TIMESTAMPDIFF()`, and `FRAC_SECOND` is now deprecated. (Bug #33834)

- **Incompatible Change:** With `ONLY_FULL_GROUP_BY` SQL mode enabled, queries such as `SELECT a FROM t1 HAVING COUNT(*) > 2` were not being rejected as they should have been.

This fix results in the following behavior:

- There is a check against mixing group and nongroup columns *only* when `ONLY_FULL_GROUP_BY` is enabled.
- This check is done both for the select list and for the `HAVING` clause if there is one.

This behavior differs from previous versions as follows:

- Previously, the `HAVING` clause was not checked when `ONLY_FULL_GROUP_BY` was enabled; now it is checked.
- Previously, the select list was checked even when `ONLY_FULL_GROUP_BY` was not enabled; now it is checked only when `ONLY_FULL_GROUP_BY` is enabled.

(Bug #31794)

- **Incompatible Change:** The MySQL 5.0.50 patch for this bug was reverted because it changed the behavior of a General Availability MySQL release. (Bug #30234)

References: See also: Bug #27525.

- **Incompatible Change:** It was possible to create a view having a column whose name consisted of an empty string or space characters only.

One result of this bug fix is that aliases for columns in the view `SELECT` statement are checked to ensure that they are legal column names. In particular, the length must be within the maximum column length of 64 characters, not the maximum alias length of 256 characters. This can cause problems for replication

or loading dump files. For additional information and workarounds, see [Restrictions on Views](#). (Bug #27695)

References: See also: Bug #31202.

- **Incompatible Change:** Several type-preserving functions and operators returned an incorrect result type that does not match their argument types: `COALESCE()`, `IF()`, `IFNULL()`, `LEAST()`, `GREATEST()`, `CASE`. These now aggregate using the precise SQL types of their arguments rather than the internal type. In addition, the result type of the `STR_TO_DATE()` function is now `DATETIME` by default. (Bug #27216)
- **Incompatible Change:** It was possible for option files to be read twice at program startup, if some of the standard option file locations turned out to be the same directory. Now duplicates are removed from the list of files to be read.

Also, users could not override system-wide settings using `~/my.cnf` because `SYSCONFDIR/my.cnf` was read last. The latter file now is read earlier so that `~/my.cnf` can override system-wide settings.

An additional correction was made to normalize directory names before adding them to the list of directories. This prevents `/etc/` and `/etc` from being considered different, for example.

The fix for this problem had a side effect such that on Unix, MySQL programs looked for options in `~/my.cnf` rather than the standard location of `~/my.cnf`. That problem is addressed in Bug #38180. (Bug #20748)

References: See also: Bug #38180.

- **Important Change; MySQL Cluster:** `AUTO_INCREMENT` columns had the following problems when used in `NDB` tables:
 - The `AUTO_INCREMENT` counter was not updated correctly when such a column was updated.
 - `AUTO_INCREMENT` values were not prefetched beyond statement boundaries.
 - `AUTO_INCREMENT` values were not handled correctly with `INSERT IGNORE` statements.
 - After being set, `ndb_autoincrement_prefetch_sz` showed a value of 1, regardless of the value it had actually been set to.
 As part of this fix, the behavior of `ndb_autoincrement_prefetch_sz` has changed. Setting this to less than 32 no longer has any effect on prefetching within statements (where IDs are now always obtained in batches of 32 or more), but only between statements. The default value for this variable has also changed, and is now 1. (Bug #25176, Bug #31956, Bug #32055)

- **Important Change; Replication:** When the master crashed during an update on a transactional table while in `autocommit` mode, the slave failed. This fix causes every transaction (including `autocommit` transactions) to be recorded in the binary log as starting with a `BEGIN` and ending with a `COMMIT` or `ROLLBACK`.



Note

The current fix does *not* cause nontransactional changes to be wrapped in `BEGIN ... COMMIT` or `BEGIN ... ROLLBACK` when written to the binary log. For this purpose, any statements affecting tables using a nontransactional storage engine such as `MyISAM` are regarded as nontransactional, even when `autocommit` is enabled.

(Bug #26395)

References: See also: Bug #29288, Bug #49522.

- **Important Change:** The server handled truncation of values having excess trailing spaces into `VARCHAR` and `TEXT` columns in different ways. This behavior has now been made consistent for columns of both of these types, and now follows the existing behavior of `VARCHAR` columns in this regard; that is, a `Note` is always issued whenever such truncation occurs.

This change does not affect columns of these types when using a binary encoding; `BLOB` columns are also unaffected by the change, since they always use a binary encoding. (Bug #30059)

- **Important Change:** When installing MySQL on AIX 5.3, you must upgrade AIX to technology level 7 (5300-07) to ensure the required thread libraries are available.
- **Important Note; Replication:** Network timeouts between the master and the slave could result in corruption of the relay log. This fix rectifies a long-standing replication issue when using unreliable networks, including replication over wide area networks such as the Internet. If you experience reliability issues and see many `You have an error in your SQL syntax` errors on replication slaves, we strongly recommend that you upgrade to a MySQL version which includes this fix. (Bug #26489)
- **MySQL Cluster:** When configured with `NDB` support, MySQL failed to compile using `gcc` 4.3 on 64bit FreeBSD systems. (Bug #34169)
- **MySQL Cluster:** The failure of a DDL statement could sometimes lead to node failures when attempting to execute subsequent DDL statements. (Bug #34160)
- **MySQL Cluster:** Extremely long `SELECT` statements (where the text of the statement was in excess of 50000 characters) against `NDB` tables returned empty results. (Bug #34107)
- **MySQL Cluster:** A periodic failure to flush the send buffer by the `NDB` TCP transporter could cause a unnecessary delay of 10 ms between operations. (Bug #34005)
- **MySQL Cluster:** When all data and SQL nodes in the cluster were shut down abnormally (that is, other than by using `STOP` in the cluster management client), `ndb_mgm` used excessive amounts of CPU. (Bug #33237)
- **MySQL Cluster:** An improperly reset internal signal was observed as a hang when using events in the `NDB` API but could result in various errors. (Bug #33206)
- **MySQL Cluster:** Incorrectly handled parameters could lead to a crash in the Transaction Coordinator during a node failure, causing other data nodes to fail. (Bug #33168)
- **MySQL Cluster:** The failure of a master node could lead to subsequent failures in local checkpointing. (Bug #32160)
- **MySQL Cluster:** An uninitialized variable in the `NDB` storage engine code led to `AUTO_INCREMENT` failures when the server was compiled with `gcc` 4.2.1. (Bug #31848)

References: This issue is a regression of: Bug #27437.

- **MySQL Cluster:** An error with an `if` statement in `sql/ha_ndbcluster.cc` could potentially lead to an infinite loop in case of failure when working with `AUTO_INCREMENT` columns in `NDB` tables. (Bug #31810)
- **MySQL Cluster:** The `NDB` storage engine code was not safe for strict-alias optimization in `gcc` 4.2.1. (Bug #31761)
- **MySQL Cluster:** Primary keys on variable-length columns (such as `VARCHAR`) did not work correctly. (Bug #31635)

- **MySQL Cluster:** Transaction atomicity was sometimes not preserved between reads and inserts under high loads. (Bug #31477)
- **MySQL Cluster:** Numerous `NDBCLUSTER` test failures occurred in builds compiled using `icc` on IA64 platforms. (Bug #31239)
- **MySQL Cluster:** Transaction timeouts were not handled well in some circumstances, leading to excessive number of transactions being aborted unnecessarily. (Bug #30379)
- **MySQL Cluster:** Having tables with a great many columns could cause Cluster backups to fail. (Bug #30172)
- **MySQL Cluster:** Issuing an `INSERT ... ON DUPLICATE KEY UPDATE` concurrently with or following a `TRUNCATE TABLE` statement on an `NDB` table failed with `NDB` error 4350 `Transaction already aborted`. (Bug #29851)
- **MySQL Cluster:** In some cases, the cluster management server logged entries multiple times following a restart of `ndb_mgmd`. (Bug #29565)
- **MySQL Cluster:** An interpreted program of sufficient size and complexity could cause all cluster data nodes to shut down due to buffer overruns. (Bug #29390)
- **MySQL Cluster:** It was possible in `config.ini` to define cluster nodes having node IDs greater than the maximum permitted value. (Bug #28298)
- **MySQL Cluster:** `UPDATE IGNORE` could sometimes fail on `NDB` tables due to the use of uninitialized data when checking for duplicate keys to be ignored. (Bug #25817)
- **MySQL Cluster:** When inserting a row into an `NDB` table with a duplicate value for a nonprimary unique key, the error issued would reference the wrong key.

This improves on an initial fix for this issue made in MySQL 5.0.30 and MySQL 5.0.33 (Bug #21072)

- **Replication:** Some kinds of internal errors, such as `Out of memory` errors, could cause the server to crash when replicating statements with user variables.
certain internal errors. (Bug #37150)
- **Replication:** `CREATE PROCEDURE` and `CREATE FUNCTION` statements containing extended comments were not written to the binary log correctly, causing parse errors on the slave. (Bug #36570)
References: See also: Bug #32575.
- **Replication:** `insert_id` was not written to the binary log for inserts into `BLACKHOLE` tables. (Bug #35178)
- **Replication:** The character sets and collations used for constant identifiers in stored procedures were not replicated correctly. (Bug #34289)
- **Replication:** A `CREATE USER`, `DROP USER`, or `RENAME USER` statement that fails on the master, or that is a duplicate of any of these statements, is no longer written to the binary log; previously, either of these occurrences could cause the slave to fail. (Bug #33862)
References: See also: Bug #29749.
- **Replication:** `SHOW BINLOG EVENTS` could fail when the binary log contained one or more events whose size was close to the value of `max_allowed_packet`. (Bug #33413)
- **Replication:** An extraneous `ROLLBACK` statement was written to the binary log by a connection that did not use any transactional tables. (Bug #33329)

- **Replication:** When a stored routine or trigger, running on a master that used MySQL 5.0 or MySQL 5.1.11 or earlier, performed an insert on an `AUTO_INCREMENT` column, the `insert_id` value was not replicated correctly to a slave running MySQL 5.1.12 or later (including any MySQL 6.0 release). (Bug #33029)

References: See also: Bug #19630.

- **Replication:** `CREATE VIEW` statements containing extended comments were not written to the binary log correctly, causing parse errors on the slave. Now, all comments are stripped from such statements before being written to the binary log. (Bug #32575)

References: See also: Bug #36570.

- **Replication:** SQL statements containing comments using `--` syntax were not replayable by `mysqlbinlog`, even though such statements replicated correctly. (Bug #32205)
- **Replication:** It was possible for the name of the relay log file to exceed the amount of memory reserved for it, possibly leading to a crash of the server. (Bug #31836)

References: See also: Bug #28597.

- **Replication:** Corruption of log events caused the server to crash on 64-bit Linux systems having 4 GB or more of memory. (Bug #31793)
- **Replication:** Use of the `@hostname` system variable in inserts in `mysql_system_tables_data.sql` did not replicate. The workaround is to select its value into a user variable (which does replicate) and insert that. (Bug #31167)
- **Replication:** `STOP SLAVE` did not stop connection attempts properly. If the I/O slave thread was attempting to connect, `STOP SLAVE` waited for the attempt to finish, sometimes for a long period of time, rather than stopping the slave immediately. (Bug #31024)

References: See also: Bug #30932.

- **Replication:** Issuing a `DROP VIEW` statement caused replication to fail if the view did not actually exist. (Bug #30998)
- **Replication:** One thread could read uninitialized memory from the stack of another thread. This issue was only known to occur in a `mysqld` process acting as both a master and a slave. (Bug #30752)
- **Replication:** Replication of `LOAD DATA INFILE` could fail when `read_buffer_size` was larger than `max_allowed_packet`. (Bug #30435)
- **Replication:** Setting `server_id` did not update its value for the current session. (Bug #28908)
- **Replication:** Due a previous change in how the default name and location of the binary log file were determined, replication failed following some upgrades. (Bug #28597, Bug #28603)

References: See also: Bug #31836. This issue is a regression of: Bug #20166.

- **Replication:** `MASTER_POS_WAIT()` did not return `NULL` when the server was not a slave. (Bug #26622)
- **Replication:** Stored procedures having `BIT` parameters were not replicated correctly. (Bug #26199)
- **Replication:** Issuing `SHOW SLAVE STATUS` as `mysqld` was shutting down could cause a crash. (Bug #26000)

- **Replication:** An `UPDATE` statement using a stored function that modified a nontransactional table was not logged if it failed. This caused the copy of the nontransactional table on the master have a row that the copy on the slave did not.

In addition, when an `INSERT ... ON DUPLICATE KEY UPDATE` statement encountered a duplicate key constraint, but the `UPDATE` did not actually change any data, the statement was not logged. As a result of this fix, such statements are now treated the same for logging purposes as other `UPDATE` statements, and so are written to the binary log. (Bug #23333)

References: See also: Bug #12713.

- **Replication:** The nonspecific error message `Wrong parameters to function register_slave` resulted when `START SLAVE` failed to register on the master due to excess length of any the slave server options `--report-host`, `--report-user`, or `--report-password`. An error message specific to each of these options is now returned in such cases. The new error messages are:

- `Failed to register slave: too long 'report-host'`
 - `Failed to register slave: too long 'report-user'`
 - `Failed to register slave; too long 'report-password'`
- (Bug #22989)

References: See also: Bug #19328.

- **Replication:** A replication slave sometimes failed to reconnect because it was unable to run `SHOW SLAVE HOSTS`. It was not necessary to run this statement on slaves (since the master should track connection IDs), and the execution of this statement by slaves was removed. (Bug #21132)

References: See also: Bug #13963, Bug #21869.

- **Replication:** `PURGE BINARY LOGS TO` and `PURGE BINARY LOGS BEFORE` did not handle missing binary log files correctly or in the same way. Now for both of these statements, if any files listed in the `.index` file are missing from the file system, the statement fails with an error. (Bug #18199, Bug #18453)
- **Replication:** `START SLAVE UNTIL MASTER_LOG_POS=position` issued on a slave that was using `--log-slave-updates` and that was involved in circular replication would cause the slave to run and stop one event later than that specified by the value of `position`. (Bug #13861)
- **Cluster API:** When reading a `BIT(64)` value using `NdbOperation::getValue()`, 12 bytes were written to the buffer rather than the expected 8 bytes. (Bug #33750)
- The fix for Bug #20748 caused a problem such that on Unix, MySQL programs looked for options in `~/my.cnf` rather than the standard location of `~/.my.cnf`. (Bug #38180)

References: See also: Bug #20748.

- The fix for Bug #33812 had the side effect of causing the `mysql` client not to be able to read some dump files produced with `mysqldump`. To address this, that fix was reverted. (Bug #38158)

References: Reverted patches: Bug #33812.

- Some binary distributions had a duplicate “-64bit” suffix in the file name. (Bug #37623)
- On Windows 64-bit systems, temporary variables of `long` types were used to store `ulong` values, causing key cache initialization to receive distorted parameters. The effect was that setting

`key_buffer_size` to values of 2GB or more caused memory exhaustion to due allocation of too much memory. (Bug #36705)

- Multiple-table `UPDATE` statements that used a temporary table could fail to update all qualifying rows or fail with a spurious duplicate-key error. (Bug #36676)
- A `REGEXP` match could return incorrect rows when the previous row matched the expression and used `CONCAT()` with an empty string. (Bug #36488)
- `mysqltest` ignored the value of `--tmpdir` in one place. (Bug #36465)
- The `mysql` client failed to recognize comment lines consisting of `--` followed by a newline. (Bug #36244)
- Conversion of a `FLOAT ZEROFILL` value to string could cause a server crash if the value was `NULL`. (Bug #36139)
- On Windows, the installer attempted to use JScript to determine whether the target data directory already existed. On Windows Vista x64, this resulted in an error because the installer was attempting to run the JScript in a 32-bit engine, which wasn't registered on Vista. The installer no longer uses JScript but instead relies on a native WiX command. (Bug #36103)
- An error in calculation of the precision of zero-length items (such as `NULL`) caused a server crash for queries that employed temporary tables. (Bug #36023)
- For `EXPLAIN EXTENDED`, execution of an uncorrelated `IN` subquery caused a crash if the subquery required a temporary table for its execution. (Bug #36011)
- The server crashed inside `NOT IN` subqueries with an impossible `WHERE` or `HAVING` clause, such as `NOT IN (SELECT ... FROM t1, t2, ... WHERE 0)`. (Bug #36005)
- Grouping or ordering of long values in unindexed `BLOB` or `TEXT` columns with the `gbk` or `big5` character set crashed the server. (Bug #35993)
- `SET GLOBAL debug=''` resulted in a Valgrind warning in `DbugParse()`, which was reading beyond the end of the control string. (Bug #35986)
- An empty bit-string literal (`b''`) caused a server crash. Now the value is parsed as an empty bit value (which is treated as an empty string in string context or 0 in numeric context). (Bug #35658)
- `mysqlbinlog` left temporary files on the disk after shutdown, leading to the pollution of the temporary directory, which eventually caused `mysqlbinlog` to fail. This caused problems in testing and other situations where `mysqlbinlog` might be invoked many times in a relatively short period of time. (Bug #35543)
- There was a memory leak when connecting to a `FEDERATED` table using a connection string that had a host value of `localhost` or omitted the host and a port value of 0 or omitted the port. (Bug #35509)
- The code for detecting a byte order mark (BOM) caused `mysql` to crash for empty input. (Bug #35480)
- Using `LOAD DATA INFILE` with a view could crash the server. (Bug #35469)
- The combination of `GROUP_CONCAT()`, `DISTINCT`, and `LEFT JOIN` could crash the server when the right table is empty. (Bug #35298)
- When a view containing a reference to `DUAL` was created, the reference was removed when the definition was stored, causing some queries against the view to fail with invalid SQL syntax errors. (Bug #35193)

- Debugging symbols were missing for some executables in Windows binary distributions. (Bug #35104)
- A query that performed a `ref_or_null` join where the second table used a key having one or columns that could be `NULL` and had a column value that was `NULL` caused the server to crash. (Bug #34945)

References: This issue is a regression of: Bug #12144.
- Some binaries produced stack corruption messages due to being built with versions of `bison` older than 2.1. Builds are now created using `bison` 2.3. (Bug #34926)
- `mysqldump` failed to return an error code when using the `--master-data` option without binary logging being enabled on the server. (Bug #34909)
- Under some circumstances, the value of `mysql_insert_id()` following a `SELECT ... INSERT` statement could return an incorrect value. This could happen when the last `SELECT ... INSERT` did not involve an `AUTO_INCREMENT` column, but the value of `mysql_insert_id()` was changed by some previous statements. (Bug #34889)
- Table and database names were mixed up in some places of the subquery transformation procedure. This could affect debugging trace output and further extensions of that procedure. (Bug #34830)
- A malformed URL used for a `FEDERATED` table's `CONNECTION` option value in a `CREATE TABLE` statement was not handled correctly and could crash the server. (Bug #34788)
- Queries such as `SELECT ROW(1, 2) IN (SELECT t1.a, 2) FROM t1 GROUP BY t1.a` (combining row constructors and subqueries in the `FROM` clause) could lead to assertion failure or unexpected error messages. (Bug #34763)
- Using `NAME_CONST()` with a negative number and an aggregate function caused MySQL to crash. This could also have a negative impact on replication. (Bug #34749)
- A memory-handling error associated with use of `GROUP_CONCAT()` in subqueries could result in a server crash. (Bug #34747)
- For an indexed integer column `col_name` and a value `N` that is one greater than the maximum value permitted for the data type of `col_name`, conditions of the form `WHERE col_name < N` failed to return rows where the value of `col_name` is `N - 1`. (Bug #34731)
- Executing a `TRUNCATE TABLE` statement on a table having both a foreign key reference and a `DELETE` trigger crashed the server. (Bug #34643)
- Some subqueries using an expression that included an aggregate function could fail or in some cases lead to a crash of the server. (Bug #34620)
- A server crash could occur if `INFORMATION_SCHEMA` tables built in memory were swapped out to disk during query execution. (Bug #34529)
- `CAST(AVG(arg) AS DECIMAL)` produced incorrect results for non-`DECIMAL` arguments. (Bug #34512)
- `mysql_explain_log` concatenated multiple-line statements, causing malformed results for statements that contained SQL comments beginning with `--`. (Bug #34339)
- Executing an `ALTER VIEW` statement on a table crashed the server. (Bug #34337)
- Several additional configuration scripts in the `BUILD` directory now are included in source distributions. These may be useful for users who wish to build MySQL from source. (See [Installing MySQL Using a Development Source Tree](#), for information about what they do.) (Bug #34291)

- Under some conditions, a `SET GLOBAL innodb_commit_concurrency` or `SET GLOBAL innodb_autoextend_increment` statement could fail. (Bug #34223)

References: This issue is a regression of: Bug #31177.

- `mysqldump` attempts to set the `character_set_results` system variable after connecting to the server. This failed for pre-4.1 servers that have no such variable, but `mysqldump` did not account for this and 1) failed to dump database contents; 2) failed to produce any error message alerting the user to the problem. (Bug #34192)
- `mysql_install_db` failed if the server was running with an SQL mode of `TRADITIONAL`. This program now resets the SQL mode internally to avoid this problem. (Bug #34159)
- For a `FEDERATED` table with an index on a nullable column, accessing the table could crash a server, return an incorrect result set, or return `ERROR 1030 (HY000): Got error 1430 from storage engine`. (Bug #33946)
- Passing anything other than an integer argument to a `LIMIT` clause in a prepared statement would fail. (This limitation was introduced to avoid replication problems; for example, replicating the statement with a string argument would cause a parse failure in the slave). Now, arguments to the `LIMIT` clause are converted to integer values, and these converted values are used when logging the statement. (Bug #33851)
- An internal buffer in `mysql` was too short. Overextending it could cause stack problems or segmentation violations on some architectures. (This is not a problem that could be exploited to run arbitrary code.) (Bug #33841)
- A query using `WHERE (column1='string1' AND column2=constant1) OR (column1='string2' AND column2=constant2)`, where `col1` used a binary collation and `string1` matched `string2` except for case, failed to match any records even when matches were found by a query using the equivalent clause `WHERE column2=constant1 OR column2=constant2`. (Bug #33833)
- The `mysql` client incorrectly parsed statements containing the word “delimiter” in mid-statement.

The fix for this bug had the side effect of causing the problem reported in Bug #38158, so it was reverted in MySQL 5.0.67. (Bug #33812)

References: See also: Bug #38158.

- Large unsigned integers were improperly handled for prepared statements, resulting in truncation or conversion to negative numbers. (Bug #33798)
- Reuse of prepared statements could cause a memory leak in the embedded server. (Bug #33796)
- The server crashed when executing a query that had a subquery containing an equality `X=Y` where `Y` referred to a named select list expression from the parent select. The server crashed when trying to use the `X=Y` equality for `ref`-based access. (Bug #33794)
- Some queries using a combination of `IN`, `CONCAT()`, and an implicit type conversion could return an incorrect result. (Bug #33764)
- In some cases a query that produced a result set when using `ORDER BY ASC` did not return any results when this was changed to `ORDER BY DESC`. (Bug #33758)
- Disabling concurrent inserts caused some cacheable queries not to be saved in the query cache. (Bug #33756)

- Use of uninitialized memory for `filesort` in a subquery caused a server crash. (Bug #33675)
- The server could crash when `REPEAT` or another control instruction was used in conjunction with labels and a `LEAVE` instruction. (Bug #33618)
- The parser permitted control structures in compound statements to have mismatched beginning and ending labels. (Bug #33618)
- `make_binary_distribution` passed the `--print-libgcc-file` option to the C compiler, but this does not work with the `ICC` compiler. (Bug #33536)
- Certain combinations of views, subselects with outer references and stored routines or triggers could cause the server to crash. (Bug #33389)
- `SET GLOBAL myisam_max_sort_file_size=DEFAULT` set `myisam_max_sort_file_size` to an incorrect value. (Bug #33382)

References: See also: Bug #31177.

- `SLEEP(0)` failed to return on 64-bit Mac OS X due to a bug in `pthread_cond_timedwait()`. (Bug #33304)
- `CREATE TABLE ... SELECT` created tables that for date columns used the obsolete `Field_date` type instead of `Field_newdate`. (Bug #33256)
- Granting the `UPDATE` privilege on one column of a view caused the server to crash. (Bug #33201)
- For `DECIMAL` columns used with the `ROUND(X,D)` or `TRUNCATE(X,D)` function with a nonconstant value of `D`, adding an `ORDER BY` for the function result produced misordered output. (Bug #33143)

References: See also: Bug #33402, Bug #30617.

- Some valid `SELECT` statements could not be used as views due to incorrect column reference resolution. (Bug #33133)
- The fix for Bug #11230 and Bug #26215 introduced a significant input-parsing slowdown for the `mysql` client. This has been corrected. (Bug #33057)

References: See also: Bug #11230, Bug #26215.

- When MySQL was built with OpenSSL, the SSL library was not properly initialized with information of which endpoint it was (server or client), causing connection failures. (Bug #33050)
- Under some circumstances a combination of aggregate functions and `GROUP BY` in a `SELECT` query over a view could lead to incorrect calculation of the result type of the aggregate function. This in turn could lead to incorrect results, or to crashes on debug builds of the server. (Bug #33049)
- For `DISTINCT` queries, MySQL 4.0 and 4.1 stopped reading joined tables as soon as the first matching row was found. However, this optimization was lost in MySQL 5.0, which instead read all matching rows. This fix for this regression may result in a major improvement in performance for `DISTINCT` queries in cases where many rows match. (Bug #32942)

- The server was built even when `configure` was run with the `--without-server` option. (Bug #32898)

References: See also: Bug #23973.

- Repeated creation and deletion of views within prepared statements could eventually crash the server. (Bug #32890)

References: See also: Bug #34587.

- `UNION` constructs cannot contain `SELECT ... INTO` except in the final `SELECT`. However, if a `UNION` was used in a subquery and an `INTO` clause appeared in the top-level query, the parser interpreted it as having appeared in the `UNION` and raised an error. (Bug #32858)
- The correct data type for a `NULL` column resulting from a `UNION` could be determined incorrectly in some cases: 1) Not correctly inferred as `NULL` depending on the number of selects; 2) Not inferred correctly as `NULL` if one select used a subquery. (Bug #32848)
- An `ORDER BY` query using `IS NULL` in the `WHERE` clause did not return correct results. (Bug #32815)
- For queries containing `GROUP_CONCAT(DISTINCT col_list ORDER BY col_list)`, there was a limitation that the `DISTINCT` columns had to be the same as `ORDER BY` columns. Incorrect results could be returned if this was not true. (Bug #32798)
- Incorrect assertions could cause a server crash for `DELETE` triggers for transactional tables. (Bug #32790)
- The `LAST_DAY()` function returns a `DATE` value, but internally the value did not have the time fields zeroed and calculations involving the value could return incorrect results. (Bug #32770)
- Use of the `cp932` character set with `CAST()` in an `ORDER BY` clause could cause a server crash. (Bug #32726)
- Inserting strings with a common prefix into a table that used the `ucs2` character set corrupted the table. (Bug #32705)
- A subquery using an `IS NULL` check of a column defined as `NOT NULL` in a table used in the `FROM` clause of the outer query produced an invalid result. (Bug #32694)
- Specifying a nonexistent column for an `INSERT DELAYED` statement caused a server crash rather than producing an error. (Bug #32676)
- Use of `CLIENT_MULTI_QUERIES` caused `libmysqld` to crash. (Bug #32624)
- The `INTERVAL()` function incorrectly handled `NULL` values in the value list. (Bug #32560)
- Use of a `NULL`-returning `GROUP BY` expression in conjunction with `WITH ROLLUP` could cause a server crash. (Bug #32558)

References: See also: Bug #31095.

- A `SELECT ... GROUP BY bit_column` query failed with an assertion if the length of the `BIT` column used for the `GROUP BY` was not an integer multiple of 8. (Bug #32556)
- Using `SELECT INTO OUTFILE` with 8-bit `ENCLOSED BY` characters led to corrupted data when the data was reloaded using `LOAD DATA INFILE`. This was because `SELECT INTO OUTFILE` failed to escape the 8-bit characters. (Bug #32533)
- For `FLUSH TABLES WITH READ LOCK`, the server failed to properly detect write-locked tables when running with low-priority updates, resulting in a crash or deadlock. (Bug #32528)
- A build problem introduced in MySQL 5.0.52 was resolved: The x86 32-bit Intel `icc`-compiled server binary had unwanted dependences on Intel `icc` runtime libraries. (Bug #32514)
- Queries using `LIKE` on tables having indexed `CHAR` columns using either of the `eucjpm`s or `ujis` character sets did not return correct results. (Bug #32510)

- The rules for valid column names were being applied differently for base tables and views. (Bug #32496)
- Sending several `KILL QUERY` statements to target a connection running `SELECT SLEEP()` could freeze the server. (Bug #32436)
- `ssl-cipher` values in option files were not being read by `libmysqlclient`. (Bug #32429)
- Repeated execution of a query containing a `CASE` expression and numerous `AND` and `OR` relations could crash the server. The root cause of the issue was determined to be that the internal `SEL_ARG` structure was not properly initialized when created. (Bug #32403)
- Referencing within a subquery an alias used in the `SELECT` list of the outer query was incorrectly permitted. (Bug #32400)
- An `ORDER BY` query on a view created using a `FEDERATED` table as a base table caused the server to crash. (Bug #32374)
- Comparison of a `BIGINT NOT NULL` column with a constant arithmetic expression that evaluated to `NULL` mistakenly caused the error `Column '...' cannot be null` (error 1048). (Bug #32335)
- Assigning a 65,536-byte string to a `TEXT` column (which can hold a maximum of 65,535 bytes) resulted in truncation without a warning. Now a truncation warning is generated. (Bug #32282)
- `MIN()` and `MAX()` could return incorrect results when an index was present if a loose index scan was used. (Bug #32268)

- Executing a prepared statement associated with a materialized cursor sent to the client a metadata packet with incorrect table and database names. The problem occurred because the server sent the name of the temporary table used by the cursor instead of the table name of the original table.

The same problem occurred when selecting from a view, in which case the name of the table name was sent, rather than the name of the view. (Bug #32265)

- Memory corruption could occur due to large index map in `Range checked for each record` status reported by `EXPLAIN SELECT`. The problem was based in an incorrectly calculated length of the buffer used to store a hexadecimal representation of an index map, which could result in buffer overrun and stack corruption under some circumstances. (Bug #32241)
- Various test program cleanups were made: 1) `mytest` and `libmysqltest` were removed. 2) `bug25714` displays an error message when invoked with incorrect arguments or the `--help` option. 3) `mysql_client_test` exits cleanly with a proper error status. (Bug #32221)
- The default grant tables on Windows contained information for host `production.mysql.com`, which should not be there. (Bug #32219)
- Under certain conditions, the presence of a `GROUP BY` clause could cause an `ORDER BY` clause to be ignored. (Bug #32202)
- For comparisons of the form `date_col OP datetime_const` (where `OP` is `=`, `<`, `>`, `<=`, or `>=`), the comparison is done using `DATETIME` values, per the fix for Bug #27590. However that fix caused any index on `date_col` not to be used and compromised performance. Now the index is used again. (Bug #32198)

References: See also: Bug #27590.

- `DATETIME` arguments specified in numeric form were treated by `DATE_ADD()` as `DATE` values. (Bug #32180)

- `InnoDB` does not support `SPATIAL` indexes, but could crash when asked to handle one. Now an error is returned. (Bug #32125)
- The server crashed on optimizations involving a join of `INT` and `MEDIUMINT` columns and a system variable in the `WHERE` clause. (Bug #32103)
- `SHOW STATUS` caused a server crash if `InnoDB` had not been initialized. (Bug #32083)
- With `lower_case_table_names` set, `CREATE TABLE LIKE` was treated differently by `libmysqld` than by the nonembedded server. (Bug #32063)
- Within a subquery, `UNION` was handled differently than at the top level, which could result in incorrect results or a server crash. (Bug #32036, Bug #32051)
- User-defined functions are not loaded if the server is started with the `--skip-grant-tables` option, but the server did not properly handle this case and issued an `Out of memory` error message instead. (Bug #32020)
- `HOUR()`, `MINUTE()`, and `SECOND()` could return nonzero values for `DATE` arguments. (Bug #31990)
- A column with malformed multibyte characters could cause the full-text parser to go into an infinite loop. (Bug #31950)
- Changing the SQL mode to cause dates with “zero” parts to be considered invalid (such as `'1000-00-00'`) could result in indexed and nonindexed searches returning different results for a column that contained such dates. (Bug #31928)
- Queries testing numeric constants containing leading zeros against `ZEROFILL` columns were not evaluated correctly. (Bug #31887)
- In debug builds, testing the result of an `IN` subquery against `NULL` caused an assertion failure. (Bug #31884)
- `mysql-test-run.pl` sometimes set up test scenarios in which the same port number was passed to multiple servers, causing one of them to be unable to start. (Bug #31880)
- Comparison results for `BETWEEN` were different from those for operators like `<` and `>` for `DATETIME`-like values with trailing extra characters such as `'2007-10-01 00:00:00 GMT-6'`. `BETWEEN` treated the values as `DATETIME`, whereas the other operators performed a binary-string comparison. Now they all uniformly use a `DATETIME` comparison, but generate warnings for values with trailing garbage. (Bug #31800)
- Name resolution for correlated subqueries and `HAVING` clauses failed to distinguish which of two was being performed when there was a reference to an outer aliased field. This could result in error messages about a `HAVING` clause for queries that had no such clause. (Bug #31797)
- If an error occurred during file creation, the server sometimes did not remove the file, resulting in an unused file in the file system. (Bug #31781)
- The server could crash during `filesort` for `ORDER BY` based on expressions with `INET_NTOA()` or `OCT()` if those functions returned `NULL`. (Bug #31758)
- The `mysqld` crash handler failed on Windows. (Bug #31745)
- For a fatal error during a filesort in `find_all_keys()`, the error was returned without the necessary handler uninitialization, causing an assertion failure. (Bug #31742)
- The examined-rows count was not incremented for `const` queries. (Bug #31700)

- The `mysql_change_user()` C API function was subject to buffer overflow. (Bug #31669)
- For `SELECT ... INTO OUTFILE`, if the `ENCLOSED BY` string is empty and the `FIELDS TERMINATED BY` string started with a special character (one of `n`, `t`, `r`, `b`, `0`, `Z`, or `N`), every occurrence of the character within field values would be duplicated. (Bug #31663)
- `SHOW COLUMNS` and `DESCRIBE` displayed `null` as the column type for a view with no valid definer. This caused `mysqldump` to produce a nonreloadable dump file for the view. (Bug #31662)
- The `mysqlbug` script did not include the correct values of `CFLAGS` and `CXXFLAGS` that were used to configure the distribution. (Bug #31644)
- `ucs2` does not work as a client character set, but attempts to use it as such were not rejected. Now `character_set_client` cannot be set to `ucs2`. This also affects statements such as `SET NAMES` and `SET CHARACTER SET`. (Bug #31615)
- The server returned the error message `Out of memory; restart server and try again` when the actual problem was that the sort buffer was too small. Now an appropriate error message is returned in such cases. (Bug #31590)
- A buffer used when setting variables was not dimensioned to accommodate the trailing `'\0'` byte, so a single-byte buffer overrun was possible. (Bug #31588)
- `HAVING` could treat lettercase of table aliases incorrectly if `lower_case_table_names` was enabled. (Bug #31562)
- The fix for Bug #24989 introduced a problem such that a `NULL` thread handler could be used during a rollback operation. This problem is unlikely to be seen in practice. (Bug #31517)
- Killing a `CREATE TABLE ... LIKE` statement that was waiting for a name lock caused a server crash. When the statement was killed, the server attempted to release locks that were not held. (Bug #31479)
- The length of the result from `IFNULL()` could be calculated incorrectly because the sign of the result was not taken into account. (Bug #31471)
- A data file required for the `ndb_restore_different_endian_data` test case was missing from binary distributions, causing the test to fail. The data file now is included. (Bug #31453, Bug #11747239)
- Queries that used the `ref` access method or index-based subquery execution over indexes that have `DECIMAL` columns could fail with an error `Column col_name cannot be null`. (Bug #31450)
- `SELECT 1 REGEX NULL` caused an assertion failure for debug servers. (Bug #31440)
- Executing `RENAME` while tables were open for use with `HANDLER` statements could cause a server crash. (Bug #31409)
- `mysql-test-run.pl` tried to create files in a directory where it could not be expected to have write permission. `mysqltest` created `.reject` files in a directory other than the one where test results go. (Bug #31398)
- `DROP USER` caused an increase in memory usage. (Bug #31347)
- For an almost-full `MyISAM` table, an insert that failed could leave the table in a corrupt state. (Bug #31305)
- `myisamchk --unpack` could corrupt a table that when unpacked has static (fixed-length) row format. (Bug #31277)

- `CONVERT(val, DATETIME)` failed on invalid input, but processing was not aborted for the `WHERE` clause, leading to a server crash. (Bug #31253)
- Allocation of an insufficiently large group-by buffer following creation of a temporary table could lead to a server crash. (Bug #31249)
- Use of `DECIMAL(n, n) ZEROFILL` in `GROUP_CONCAT()` could cause a server crash. (Bug #31227)
- When sorting privilege table rows, the server treated escaped wildcard characters (`\%` and `_`) the same as unescaped wildcard characters (`%` and `_`), resulting in incorrect row ordering. (Bug #31194)
- Server variables could not be set to their current values on Linux platforms. (Bug #31177)

References: See also: Bug #6958.

- With small values of `myisam_sort_buffer_size`, `REPAIR TABLE` for `MyISAM` tables could cause a server crash. (Bug #31174)
- If `MAKETIME()` returned `NULL` when used in an `ORDER BY` that was evaluated using `filesort`, a server crash could result. (Bug #31160)
- Full-text searches on `ucs2` columns caused a server crash. (`FULLTEXT` indexes on `ucs2` columns cannot be used, but it should be possible to perform `IN BOOLEAN MODE` searches on `ucs2` columns without a crash.) (Bug #31159)
- Data in `BLOB` or `GEOMETRY` columns could be cropped when performing a `UNION` query. (Bug #31158)
- An assertion designed to detect a bug in the `ROLLUP` implementation would incorrectly be triggered when used in a subquery context with noncacheable statements. (Bug #31156)
- Selecting spatial types in a `UNION` could cause a server crash. (Bug #31155)
- Use of `GROUP_CONCAT(DISTINCT bit_column)` caused an assertion failure. (Bug #31154)
- The server crashed in the parser when running out of memory. Memory handling in the parser has been improved to gracefully return an error when out-of-memory conditions occur in the parser. (Bug #31153)
- MySQL declares a `UNIQUE` key as a `PRIMARY` key if it doesn't have `NULL` columns and is not a partial key, and the `PRIMARY` key must always be the first key. However, in some cases, a nonfirst key could be reported as `PRIMARY`, leading to an assert failure by `InnoDB`. This is fixed by correcting the key sort order. (Bug #31137)
- `GROUP BY NULL WITH ROLLUP` could cause a server crash. (Bug #31095)

References: See also: Bug #32558.

- `REGEXP` operations could cause a server crash for character sets such as `ucs2`. Now the arguments are converted to `utf8` if possible, to permit correct results to be produced if the resulting strings contain only 8-bit characters. (Bug #31081)
- Internal conversion routines could fail for several multibyte character sets (`big5`, `cp932`, `euckr`, `gb2312`, `sjis`) for empty strings or during evaluation of `SOUNDS LIKE`. (Bug #31069, Bug #31070)
- Many nested subqueries in a single query could led to excessive memory consumption and possibly a crash of the server. (Bug #31048)
- The `MOD()` function and the `%` operator crashed the server for a divisor less than 1 with a very long fractional part. (Bug #31019)

- On Windows, the `pthread_mutex_trylock()` implementation was incorrect. (Bug #30992)
- A character set introducer followed by a hexadecimal or bit-value literal did not check its argument and could return an ill-formed result for invalid input. (Bug #30986)
- `CHAR(str USING charset)` did not check its argument and could return an ill-formed result for invalid input. (Bug #30982)
- The result from `CHAR(str USING ucs2)` did not add a leading 0x00 byte for input strings with an odd number of bytes. (Bug #30981)
- On Windows, `SHOW PROCESSLIST` could display process entries with a `State` value of `*** DEAD ***`. (Bug #30960)
- The `GeomFromText()` function could cause a server crash if the first argument was `NULL` or the empty string. (Bug #30955)
- `MAKEDATE()` incorrectly moved year values in the 100 to 200 range into the 1970 to 2069 range. (This is legitimate for 00 to 99, but three-digit years should be used unchanged.) (Bug #30951)
- When invoked with constant arguments, `STR_TO_DATE()` could use a cached value for the format string and return incorrect results. (Bug #30942)
- `GROUP_CONCAT()` returned `' , '` rather than an empty string when the argument column contained only empty strings. (Bug #30897)
- `ROUND(X,D)` or `TRUNCATE(X,D)` for nonconstant values of `D` could crash the server if these functions were used in an `ORDER BY` that was resolved using `filesort`. (Bug #30889)
- For `MEMORY` tables, lookups for `NULL` values in `BTREE` indexes could return incorrect results. (Bug #30885)
- Calling `NAME_CONST()` with nonconstant arguments triggered an assertion failure. Nonconstant arguments are no longer permitted. (Bug #30832)
- For a spatial column with a regular (non-`SPATIAL`) index, queries failed if the optimizer tried to use the index. (Bug #30825)
- Values for the `--tc-heuristic-recover` option incorrectly were treated as values for the `--myisam-stats-method` option. (Bug #30821)
- The optimizer incorrectly optimized conditions out of the `WHERE` clause in some queries involving subqueries and indexed columns. (Bug #30788)
- If an alias was used to refer to the value returned by a stored function within a subselect, the outer select recognized the alias but failed to retrieve the value assigned to it in the subselect. (Bug #30787)

References: This issue is a regression of: Bug #20777.

- Improper calculation of `CASE` expression results could lead to value truncation. (Bug #30782)
- On Windows, the `pthread_mutex_trylock()` implementation was incorrect. One symptom was that invalidating the query cache could cause a server crash. (Bug #30768)
- A multiple-table `UPDATE` involving transactional and nontransactional tables caused an assertion failure. (Bug #30763)
- Under some circumstances, `CREATE TABLE ... SELECT` could crash the server or incorrectly report that the table row size was too large. (Bug #30736)

- Using the `MIN()` or `MAX()` function to select one part of a multi-part key could cause a crash when the function result was `NULL`. (Bug #30715)
- The optimizer could ignore `ORDER BY` in cases when the result set is ordered by `filesort`, resulting in rows being returned in incorrect order. (Bug #30666)
- `MyISAM` tables could not exceed 4294967295 ($2^{32} - 1$) rows on Windows. (Bug #30638)
- `mysql-test-run.pl` could not run `mysqld` with `root` privileges. (Bug #30630)
- Binary logging for a stored procedure differed depending on whether or not execution occurred in a prepared statement. (Bug #30604)
- For `MEMORY` tables, `DELETE` statements that remove rows based on an index read could fail to remove all matching rows. (Bug #30590)
- Using `GROUP BY` on an expression of the form `timestamp_col DIV number` caused a server crash due to incorrect calculation of number of decimals. (Bug #30587)
- The options available to the `CHECK TABLE` statement were also permitted in `OPTIMIZE TABLE` and `ANALYZE TABLE` statements, but caused corruption during their execution. These options were never supported for these statements, and an error is now raised if you try to apply these options to these statements. (Bug #30495)
- When expanding a `*` in a `USING` or `NATURAL` join, the check for table access for both tables in the join was done using only the grant information of the first table. (Bug #30468)
- When casting a string value to an integer, cases where the input string contained a decimal point and was long enough to overrun the `unsigned long long` type were not handled correctly. The position of the decimal point was not taken into account which resulted in miscalculated numbers and incorrect truncation to appropriate SQL data type limits. (Bug #30453)
- Versions of `mysqldump` from MySQL 4.1 or higher tried to use `START TRANSACTION WITH CONSISTENT SNAPSHOT` if the `--single-transaction` and `--master-data` options were given, even with servers older than 4.1 that do not support consistent snapshots. (Bug #30444)
- For `CREATE ... SELECT ... FROM`, where the resulting table contained indexes, adding `SQL_BUFFER_RESULT` to the `SELECT` part caused index corruption in the table. (Bug #30384)
- An orphaned PID file from a no-longer-running process could cause `mysql.server` to wait for that process to exit even though it does not exist. (Bug #30378)
- The optimizer made incorrect assumptions about the value of the `is_member` value for user-defined functions, sometimes resulting in incorrect ordering of UDF results. (Bug #30355)
- Some valid `euc-kr` characters having the second byte in the ranges `[0x41..0x5A]` and `[0x61..0x7A]` were rejected. (Bug #30315)
- Simultaneous `ALTER TABLE` statements for `BLACKHOLE` tables caused 100% CPU use due to locking problems. (Bug #30294)
- Setting certain values on a table using a spatial index could cause the server to crash. (Bug #30286)
- Tables with a `GEOMETRY` column could be marked as corrupt if you added a non-`SPATIAL` index on a `GEOMETRY` column. (Bug #30284)
- Some `INFORMATION_SCHEMA` tables are intended for internal use, but could be accessed by using `SHOW` statements. (Bug #30079)

- On some 64-bit systems, inserting the largest negative value into a `BIGINT` column resulted in incorrect data. (Bug #30069)
- Under some circumstances, a UDF initialization function could be passed incorrect argument lengths. (Bug #29804)
- Specifying the `--without-geometry` option for `configure` caused server compilation to fail. (Bug #29772)
- `configure` did not find `nss` on some Linux platforms. (Bug #29658)
- The `mysql_config` command would output `CFLAGS` values that were incompatible with C++ for the HP-UX platform. (Bug #29645)
- Views were treated as insertable even if some base table columns with no default value were omitted from the view definition. (This is contrary to the condition for insertability that a view must contain all columns in the base table that do not have a default value.) (Bug #29477)
- The `mysql` client program now ignores Unicode byte order mark (BOM) characters at the beginning of input files. Previously, it read them and sent them to the server, resulting in a syntax error.

Presence of a BOM does not cause `mysql` to change its default character set. To do that, invoke `mysql` with an option such as `--default-character-set=utf8`. (Bug #29323)

- For transactional tables, an error during a multiple-table `DELETE` statement did not roll back the statement. (Bug #29136)
- The `log` and `log_slow_queries` system variables were displayed by `SHOW VARIABLES` but could not be accessed in expressions as `@@log` and `@@log_slow_queries`. Also, attempting to set them with `SET` produced an incorrect `Unknown system variable` message. Now these variables can be accessed in expressions and attempting to set their values produces an error message that the variable is read only. (Bug #29131)
- Denormalized double-precision numbers cannot be handled properly by old MIPS processors. For IRIX, this is now handled by enabling a mode to use a software workaround. (Bug #29085)
- `SHOW VARIABLES` did not display the `relay_log`, `relay_log_index`, or `relay_log_info_file` system variables. (Bug #28893)
- The MySQL preferences pane did not work to start or stop MySQL on Mac OS X 10.5 (Leopard). (Bug #28854)
- When doing a `DELETE` on a table that involved a `JOIN` with `MyISAM` or `MERGE` tables and the `JOIN` referred to the same table, the operation could fail reporting `ERROR 1030 (HY000): Got error 134 from storage engine`. This was because scans on the table contents would change because of rows that had already been deleted. (Bug #28837)
- On Windows, `mysql_upgrade` created temporary files in `C:\` and did not clean them up. (Bug #28774)
- Index hints specified in view definitions were ignored when using the view to select from the base table. (Bug #28702)
- Views do not have indexes, so index hints do not apply. Use of index hints when selecting from a view is no longer permitted. (Bug #28701)
- After changing the SQL mode to a restrictive value that would make already inserted dates in a column be considered invalid, searches returned different results depending on whether the column was indexed. (Bug #28687)

- For upgrading to a new major version using RPM packages (such as 4.1 to 5.0), if the installation procedure found an existing MySQL server running, it could fail to shut down the old server, but also erroneously removed the server's socket file. Now the procedure checks for an existing server package from a different vendor or major MySQL version. In such case, it refuses to install the server and recommends how to safely remove the old packages before installing the new ones. (Bug #28555)
- The result from `CHAR()` was incorrectly assumed in some contexts to return a single-byte result. (Bug #28550)
- `mysqlhotcopy` silently skipped databases with names consisting of two alphanumeric characters. (Bug #28460)
- The parser confused user-defined function (UDF) and stored function creation for `CREATE FUNCTION` and required that there be a default database when creating UDFs, although there is no such requirement. (Bug #28318, Bug #29816)
- The SQL parser did not accept an empty `UNION=()` clause. This meant that, when there were no underlying tables specified for a `MERGE` table, `SHOW CREATE TABLE` and `mysqldump` both output statements that could not be executed.

Now it is possible to execute a `CREATE TABLE` or `ALTER TABLE` statement with an empty `UNION=()` clause. However, `SHOW CREATE TABLE` and `mysqldump` do not output the `UNION=()` clause if there are no underlying tables specified for a `MERGE` table. This also means it is now possible to remove the underlying tables for a `MERGE` table using `ALTER TABLE ... UNION=()`. (Bug #28248)

- The result of a comparison between `VARBINARY` and `BINARY` columns differed depending on whether the `VARBINARY` column was indexed. (Bug #28076)
- The metadata in some `MYSQL_FIELD` members could be incorrect when a temporary table was used to evaluate a query. (Bug #27990)
- An `ORDER BY` at the end of a `UNION` affected individual `SELECT` statements rather than the overall query result. (Bug #27848)
- `comp_err` created files with permissions such that they might be inaccessible during `make install` operations. (Bug #27789)
- It was possible to exhaust memory by repeatedly running `index_merge` queries and never performing any `FLUSH TABLES` statements. (Bug #27732)
- The anonymous accounts were not being created during MySQL installation. (Bug #27692)
- When `utf8` was set as the connection character set, using `SPACE()` with a non-Unicode column produced an error. (Bug #27580)

References: See also: Bug #23637.

- A race condition between killing a statement and the thread executing the statement could lead to a situation such that the binary log contained an event indicating that the statement was killed, whereas the statement actually executed to completion. (Bug #27571)
- Some queries using the `NAME_CONST()` function failed to return either a result or an error to the client, causing it to hang. This was due to the fact that there was no check to insure that both arguments to this function were constant expressions. (Bug #27545, Bug #32559)
- With the `read_only` system variable enabled, `CREATE DATABASE` and `DROP DATABASE` were permitted to users who did not have the `SUPER` privilege. (Bug #27440)

- `resolveip` failed to produce correct results for host names that begin with a digit. (Bug #27427)
- In `ORDER BY` clauses, mixing aggregate functions and nongrouping columns is not permitted if the `ONLY_FULL_GROUP_BY` SQL mode is enabled. However, in some cases, no error was thrown because of insufficient checking. (Bug #27219)
- For the `--record_log_pos` option, `mysqlhotcopy` now determines the slave status information from the result of `SHOW SLAVE STATUS` by using the `Relay_Master_Log_File` and `Exec_Master_Log_Pos` values rather than the `Master_Log_File` and `Read_Master_Log_Pos` values. This provides a more accurate indication of slave execution relative to the master. (Bug #27101)
- The MySQL Instance Configuration Wizard would not permit you to choose a service name, even though the criteria for the service name were valid. The code that checks the name has been updated to support the correct criteria of any string less than 256 character and not containing either a forward or backward slash character. (Bug #27013)
- `mysqld` sometimes miscalculated the number of digits required when storing a floating-point number in a `CHAR` column. This caused the value to be truncated, or (when using a debug build) caused the server to crash. (Bug #26788)

References: See also: Bug #12860.

- `config-win.h` unconditionally defined `bool` as `BOOL`, causing problems on systems where `bool` is 1 byte and `BOOL` is 4 bytes. (Bug #26461)
- The internal `init_time()` library function was renamed to `my_init_time()` to avoid conflicts with external libraries. (Bug #26294)
- On Windows, for distributions built with debugging support, `mysql` could crash if the user typed **Control +C**. (Bug #26243)
- `mysqlcheck -A -r` did not correctly identify all tables that needed repairing. (Bug #25347)
- On Windows, an error in `configure.js` caused installation of source distributions to fail. (Bug #25340)
- Using `mysqldump` in MySQL 5.1 resulted in dump files that could not be loaded in MySQL 5.0 because `USING type_name` options in index definitions appeared after the index column list, whereas 5.0 accepted only the old syntax that has `USING` before the column list. The parser in 5.0 now accepts `USING` following the column list. (Bug #25162)
- The client library had no way to return an error if no connection had been established. This caused problems such as `mysql_library_init()` failing silently if no `errmsg.sys` file was available. (Bug #25097)
- On Mac OS X, the StartupItem for MySQL did not work. (Bug #25008)
- For Windows 64-bit builds, enabling shared-memory support caused client connections to fail. (Bug #24992)
- If the expected precision of an arithmetic expression exceeded the maximum precision supported by MySQL, the precision of the result was reduced by an unpredictable or arbitrary amount, rather than to the maximum precision. In some cases, exceeding the maximum supported precision could also lead to a crash of the server. (Bug #24907)
- `mysql` did not use its completion table. Also, the table contained few entries. (Bug #24624)
- If a user installed MySQL Server and set a password for the `root` user, and then uninstalled and reinstalled MySQL Server to the same location, the user could not use the MySQL Instance Config

wizard to configure the server because the uninstall operation left the previous data directory intact. The config wizard *assumed* that any new install (not an upgrade) would have the default data directory where the `root` user has no password. The installer now writes a registry key named `FoundExistingDataDir`. If the installer finds an existing data directory, the key will have a value of 1, otherwise it will have a value of 0. When `MySQLInstanceConfig.exe` is run, it will attempt to read the key. If it can read the key, and the value is 1 and there is no existing instance of the server (indicating a new installation), the Config Wizard will permit the user to input the old password so the server can be configured. (Bug #24215)

- The MySQL header files contained some duplicate macro definitions that could cause compilation problems. (Bug #23839)
- `SHOW COLUMNS` on a `TEMPORARY` table caused locking issues. (Bug #23588)
- For distributions compiled with the bundled `libedit` library, there were difficulties using the `mysql` client to enter input for non-ASCII or multibyte characters. (Bug #23097)
- For Windows Vista, `MySQLInstanceConfig.exe` did not include a proper manifest enabling it to run with administrative privileges. (Bug #22563)

References: See also: Bug #24732.

- Using `FLUSH TABLES` in one connection while another connection is using `HANDLER` statements caused a server crash.



Note

This fix supersedes a fix made previously in MySQL 5.0.32 and reverted in MySQL 5.0.48.

(Bug #21587)

References: See also: Bug #29474.

- On Mac OS X, `mysqld` did not react to Control+C when run under `gdb`, even when run with the `--gdb` option. (Bug #21567)
- `mysql_config` output did not include `-lmygcc` on some platforms when it was needed. (Bug #21158)
- `mysql-stress-test.pl` and `mysqld_multi.server.sh` were missing from some binary distributions. (Bug #21023, Bug #25486)
- `mysqldumpslow` returned a confusing error message when no configuration file was found. (Bug #20455)
- Host names sometimes were treated as case sensitive in account-management statements (`CREATE USER`, `GRANT`, `REVOKE`, and so forth). (Bug #19828)
- The `readline` library has been updated to version 5.2. This addresses issues in the `mysql` client where history and editing within the client failed to work as expected. (Bug #18431)
- The `Aborted_clients` status variable was incremented twice if a client exited without calling `mysql_close()`. (Bug #16918)
- The parser used signed rather than unsigned values in some cases that caused legal lengths in column declarations to be rejected. (Bug #15776)
- A `SET` column whose definition specified 64 elements could not be updated using integer values. (Bug #15409)

- Clients were ignoring the TCP/IP port number specified as the default port using the `--with-tcp-port` configuration option. (Bug #15327)
- Zero-padding of exponent values was not the same across platforms. (Bug #12860)
- Values of types `REAL ZEROFILL`, `DOUBLE ZEROFILL`, `FLOAT ZEROFILL`, were not zero-filled when converted to a character representation in the C prepared statement API. (Bug #11589)
- `mysql` stripped comments from statements sent to the server. Now the `--comments` or `--skip-comments` option can be used to control whether to retain or strip comments. The default is `--skip-comments`. (Bug #11230, Bug #26215)
- If an `INSERT ... SELECT` statement is executed, and no automatically generated value is successfully inserted, then `mysql_insert_id()` returns the ID of the last inserted row.

If no automatically generated value is successfully inserted, then `mysql_insert_id()` returns 0. (Bug #9481)

- `MySQLInstanceConfig.exe` did not save the `innodb_data_home_dir` value to the `my.ini` file under certain circumstances. (Bug #6627)
- Several buffer-size system variables were either being handled incorrectly for large values (for settings larger than 4GB, they were truncated to values less than 4GB without a warning), or were limited unnecessarily to 4GB even on 64-bit systems. The following changes were made:
 - For `key_buffer_size`, values larger than 4GB are permitted on 64-bit platforms (except Windows, for which large values are truncated to 4GB with a warning).
 - For `join_buffer_size`, `sort_buffer_size`, and `myisam_sort_buffer_size`, values are limited to 4GB on all platforms. Larger values are truncated to 4GB with a warning.

In addition, settings for `read_buffer_size` and `read_rnd_buffer_size` are limited to 2GB on all platforms. Larger values are truncated to 2GB with a warning. (Bug #5731, Bug #29419, Bug #29446)

- Executing `DISABLE KEYS` and `ENABLE KEYS` on a nonempty table would cause the size of the index file for the table to be considerable. This was because the `DISABLE KEYS` operation would only mark the existing index, without deleting the index blocks. The `ENABLE KEYS` operation would re-create the index, adding new blocks, while the previous index blocks would remain. Existing indexes are now dropped and recreated when the `ENABLE KEYS` statement is executed. (Bug #4692)

Changes in MySQL Enterprise 5.0.66sp1 [QSP] (2008-10-23)

This is a *Service Pack* release of the MySQL Enterprise Server 5.0.

This section documents all changes and bugfixes that have been applied since the last MySQL Enterprise Server release (5.0.66a).

If you would like to receive more fine-grained and personalized *update alerts* about fixes that are relevant to the version and features you use, please consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details please see <http://www.mysql.com/products/enterprise/advisors.html>.

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- **Security Enhancement:** To enable stricter control over the location from which user-defined functions can be loaded, the `plugin_dir` system variable has been backported from MySQL 5.1. If the value is nonempty, user-defined function object files can be loaded only from the directory named by this variable. If the value is empty, the behavior that is used prior to the inclusion of `plugin_dir` applies: The UDF object files must be located in a directory that is searched by your system's dynamic linker.

If the plugin directory is writable by the server, it may be possible for a user to write executable code to a file in the directory using `SELECT ... INTO DUMPFILE`. This can be prevented by making `plugin_dir` read only to the server or by setting `--secure-file-priv` to a directory where `SELECT` writes can be made safely. (Bug #37428)

Bugs Fixed

- **Security Fix; Important Change:** It was possible to circumvent privileges through the creation of `MyISAM` tables employing the `DATA DIRECTORY` and `INDEX DIRECTORY` options to overwrite existing table files in the MySQL data directory. Use of the MySQL data directory in `DATA DIRECTORY` and `INDEX DIRECTORY` path name is no longer permitted.

Additional corrections were made to handle the data directory path name if it contains symlinked directories in its path, and to make the check both at table-creation time and at table-opening time later. (Bug #32167, CVE-2008-2079)

References: See also: Bug #39277.

- **Security Enhancement:** The server consumed excess memory while parsing statements with hundreds or thousands of nested boolean conditions (such as `OR (OR ... (OR ...))`). This could lead to a server crash or incorrect statement execution, or cause other client statements to fail due to lack of memory. The latter result constitutes a denial of service. (Bug #38296)

Changes in MySQL Enterprise 5.0.66a [MRU] (2008-07-16)

This is a *Monthly Rapid Update* release of the MySQL Enterprise Server 5.0.

This is a bugfix release that replaces MySQL 5.0.66.

Bugs Fixed

- The fix for Bug #20748 caused a problem such that on Unix, MySQL programs looked for options in `~/my.cnf` rather than the standard location of `~/my.cnf`. (Bug #38180)

References: See also: Bug #20748.

Changes in MySQL Enterprise 5.0.66 [MRU] (2008-07-09)

This is a *Monthly Rapid Update* release of the MySQL Enterprise Server 5.0.

This section documents all changes and bugfixes that have been applied since the last MySQL Enterprise Server release (5.0.64). If you would like to receive more fine-grained and personalized *update alerts* about fixes that are relevant to the version and features you use, please consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details please see <http://www.mysql.com/products/enterprise/advisors.html>.



Important

This release was withdrawn from production due to the side effect produced by Bug #20748. It has been replaced by MySQL 5.0.66a, which should be used instead.

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- `mysql-test-run.pl` now supports `--client-bindir` and `--client-libdir` options for specifying the directory where client binaries and libraries are located. (Bug #34995)

Bugs Fixed

- **Incompatible Change:** An additional correction to the original MySQL 5.0.64 fix was made to normalize directory names before adding them to the list of directories. This prevents `/etc/` and `/etc` from being considered different, for example. (Bug #20748)

References: See also: Bug #38180.

- **Replication:** Some kinds of internal errors, such as `Out of memory` errors, could cause the server to crash when replicating statements with user variables.
certain internal errors. (Bug #37150)
- Some binary distributions had a duplicate “-64bit” suffix in the file name. (Bug #37623)
- The `mysql` client failed to recognize comment lines consisting of `--` followed by a newline. (Bug #36244)
- An empty bit-string literal (`b''`) caused a server crash. Now the value is parsed as an empty bit value (which is treated as an empty string in string context or 0 in numeric context). (Bug #35658)
- `mysqlbinlog` left temporary files on the disk after shutdown, leading to the pollution of the temporary directory, which eventually caused `mysqlbinlog` to fail. This caused problems in testing and other situations where `mysqlbinlog` might be invoked many times in a relatively short period of time. (Bug #35543)
- The code for detecting a byte order mark (BOM) caused `mysql` to crash for empty input. (Bug #35480)
- The `mysql` client incorrectly parsed statements containing the word “delimiter” in mid-statement.

The fix for this bug had the side effect of causing the problem reported in Bug #38158, so it was reverted in MySQL 5.0.67. (Bug #33812)

References: See also: Bug #38158.

Changes in MySQL Enterprise 5.0.64 [MRU] (2008-06-10)

This is a *Monthly Rapid Update* release of the MySQL Enterprise Server 5.0.

This section documents all changes and bugfixes that have been applied since the last MySQL Enterprise Server release (5.0.62). If you would like to receive more fine-grained and personalized *update alerts* about fixes that are relevant to the version and features you use, please consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details please see <http://www.mysql.com/products/enterprise/advisors.html>.

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- **Incompatible Change; Important Change:** The `FEDERATED` storage engine is now disabled by default in the `.cnf` files shipped with MySQL distributions (`my-huge.cnf`, `my-medium.cnf`, and so forth). This affects server behavior only if you install one of these files. (Bug #37069)

Bugs Fixed

- **Replication:** `CREATE PROCEDURE` and `CREATE FUNCTION` statements containing extended comments were not written to the binary log correctly, causing parse errors on the slave. (Bug #36570)

References: See also: Bug #32575.

- On Windows 64-bit systems, temporary variables of `long` types were used to store `ulong` values, causing key cache initialization to receive distorted parameters. The effect was that setting `key_buffer_size` to values of 2GB or more caused memory exhaustion to due allocation of too much memory. (Bug #36705)
- Multiple-table `UPDATE` statements that used a temporary table could fail to update all qualifying rows or fail with a spurious duplicate-key error. (Bug #36676)
- A `REGEXP` match could return incorrect rows when the previous row matched the expression and used `CONCAT()` with an empty string. (Bug #36488)
- For `EXPLAIN EXTENDED`, execution of an uncorrelated `IN` subquery caused a crash if the subquery required a temporary table for its execution. (Bug #36011)

Changes in MySQL Enterprise 5.0.62 [MRU] (2008-05-12)

This is a *Monthly Rapid Update* release of the MySQL Enterprise Server 5.0.

This section documents all changes and bugfixes that have been applied since the last MySQL Enterprise Server release (5.0.60). If you would like to receive more fine-grained and personalized *update alerts* about fixes that are relevant to the version and features you use, please consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details please see <http://www.mysql.com/products/enterprise/advisors.html>.

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- **Important Change:** Some changes were made to `CHECK TABLE ... FOR UPGRADE` and `REPAIR TABLE` with respect to detection and handling of tables with incompatible `.frm` files (files created with a different version of the MySQL server). These changes also affect `mysqlcheck` because that program uses `CHECK TABLE` and `REPAIR TABLE`, and thus also `mysql_upgrade` because that program invokes `mysqlcheck`.
 - If your table was created by a different version of the MySQL server than the one you are currently running, `CHECK TABLE ... FOR UPGRADE` indicates that the table has an `.frm` file with an incompatible version. In this case, the result set returned by `CHECK TABLE` contains a line with a `Msg_type` value of `error` and a `Msg_text` value of `Table upgrade required. Please do "REPAIR TABLE `tbl_name`" to fix it!`
 - `REPAIR TABLE` without `USE_FRM` upgrades the `.frm` file to the current version.

- If you use `REPAIR TABLE ...USE_FRM` and your table was created by a different version of the MySQL server than the one you are currently running, `REPAIR TABLE` will not attempt to repair the table. In this case, the result set returned by `REPAIR TABLE` contains a line with a `Msg_type` value of `error` and a `Msg_text` value of `Failed repairing incompatible .FRM file`.

Previously, use of `REPAIR TABLE ...USE_FRM` with a table created by a different version of the MySQL server risked the loss of all rows in the table.

(Bug #36055)

- `mysql_upgrade` now has a `--tmpdir` option to enable the location of temporary files to be specified. (Bug #36469)

Bugs Fixed

- **Important Change:** The server no longer issues warnings for truncation of excess spaces for values inserted into `CHAR` columns. This reverts a change in the previous release that caused warnings to be issued. (Bug #30059)
- **Replication:** `CREATE VIEW` statements containing extended comments were not written to the binary log correctly, causing parse errors on the slave. Now, all comments are stripped from such statements before being written to the binary log. (Bug #32575)

References: See also: Bug #36570.

- `mysqltest` ignored the value of `--tmpdir` in one place. (Bug #36465)
- Conversion of a `FLOAT ZEROFILL` value to string could cause a server crash if the value was `NULL`. (Bug #36139)
- An error in calculation of the precision of zero-length items (such as `NULL`) caused a server crash for queries that employed temporary tables. (Bug #36023)
- The server crashed inside `NOT IN` subqueries with an impossible `WHERE` or `HAVING` clause, such as `NOT IN (SELECT ... FROM t1, t2, ... WHERE 0)`. (Bug #36005)
- Grouping or ordering of long values in unindexed `BLOB` or `TEXT` columns with the `gbk` or `big5` character set crashed the server. (Bug #35993)
- `SET GLOBAL debug=''` resulted in a Valgrind warning in `DbugParse()`, which was reading beyond the end of the control string. (Bug #35986)
- The combination of `GROUP_CONCAT()`, `DISTINCT`, and `LEFT JOIN` could crash the server when the right table is empty. (Bug #35298)
- Several additional configuration scripts in the `BUILD` directory now are included in source distributions. These may be useful for users who wish to build MySQL from source. (See [Installing MySQL Using a Development Source Tree](#), for information about what they do.) (Bug #34291)
- The internal `init_time()` library function was renamed to `my_init_time()` to avoid conflicts with external libraries. (Bug #26294)
- The parser used signed rather than unsigned values in some cases that caused legal lengths in column declarations to be rejected. (Bug #15776)

Changes in MySQL Enterprise 5.0.60sp1 [QSP] (2008-06-27)

This is a *Service Pack* release of the MySQL Enterprise Server 5.0.

This section documents all changes and bugfixes that have been applied since the last MySQL Enterprise Server release (5.0.60).

If you would like to receive more fine-grained and personalized *update alerts* about fixes that are relevant to the version and features you use, please consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details please see <http://www.mysql.com/products/enterprise/advisors.html>.

Version 5.0.60sp1 has no changelog entries, or they have not yet been published because the product version has not yet been released.

Changes in MySQL Enterprise 5.0.60 [MRU] (2008-04-28)

This is a *Monthly Rapid Update* release of the MySQL Enterprise Server 5.0.

This section documents all changes and bugfixes that have been applied since the last MySQL Enterprise Server release (5.0.58). If you would like to receive more fine-grained and personalized *update alerts* about fixes that are relevant to the version and features you use, please consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details please see <http://www.mysql.com/products/enterprise/advisors.html>.

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- For binary `.tar.gz` packages, `mysqld` and other binaries now are compiled with debugging symbols included to enable easier use with a debugger. If you do not need debugging symbols and are short on disk space, you can use `strip` to remove the symbols from the binaries. (Bug #33252)

Bugs Fixed

- **Security Fix; Important Change:** It was possible to circumvent privileges through the creation of `MyISAM` tables employing the `DATA DIRECTORY` and `INDEX DIRECTORY` options to overwrite existing table files in the MySQL data directory. Use of the MySQL data directory in `DATA DIRECTORY` and `INDEX DIRECTORY` path name is no longer permitted.



Note

Additional fixes were made in MySQL 5.0.70.

(Bug #32167, CVE-2008-2079)

References: See also: Bug #39277.

- **Incompatible Change:** It was possible to use `FRAC_SECOND` as a synonym for `MICROSECOND` with `DATE_ADD()`, `DATE_SUB()`, and `INTERVAL`; now, using `FRAC_SECOND` with anything other than `TIMESTAMPADD()` or `TIMESTAMPDIFF()` produces a syntax error.

It is now possible (and preferable) to use `MICROSECOND` with `TIMESTAMPADD()` and `TIMESTAMPDIFF()`, and `FRAC_SECOND` is now deprecated. (Bug #33834)

- **Important Change:** The server handled truncation of values having excess trailing spaces into `CHAR`, `VARCHAR`, and `TEXT` columns in different ways. This behavior has now been made consistent for columns of all three of these types, and now follows the existing behavior of `VARCHAR` columns in this regard; that is, a [Note](#) is always issued whenever such truncation occurs.

This change does not affect columns of these three types when using a binary encoding; `BLOB` columns are also unaffected by the change, since they always use a binary encoding. (Bug #30059)

- **Replication:** `insert_id` was not written to the binary log for inserts into `BLACKHOLE` tables. (Bug #35178)
- **Replication:** The character sets and collations used for constant identifiers in stored procedures were not replicated correctly. (Bug #34289)
- **Replication:** An extraneous `ROLLBACK` statement was written to the binary log by a connection that did not use any transactional tables. (Bug #33329)
- **Replication:** When a stored routine or trigger, running on a master that used MySQL 5.0 or MySQL 5.1.11 or earlier, performed an insert on an `AUTO_INCREMENT` column, the `insert_id` value was not replicated correctly to a slave running MySQL 5.1.12 or later (including any MySQL 6.0 release). (Bug #33029)

References: See also: Bug #19630.

- **Replication:** `STOP SLAVE` did not stop connection attempts properly. If the I/O slave thread was attempting to connect, `STOP SLAVE` waited for the attempt to finish, sometimes for a long period of time, rather than stopping the slave immediately. (Bug #31024)

References: See also: Bug #30932.

- **Replication:** `MASTER_POS_WAIT()` did not return `NULL` when the server was not a slave. (Bug #26622)
- **Replication:** The nonspecific error message `Wrong parameters to function register_slave` resulted when `START SLAVE` failed to register on the master due to excess length of any the slave server options `--report-host`, `--report-user`, or `--report-password`. An error message specific to each of these options is now returned in such cases. The new error messages are:

- `Failed to register slave: too long 'report-host'`
 - `Failed to register slave: too long 'report-user'`
 - `Failed to register slave; too long 'report-password'`
- (Bug #22989)

References: See also: Bug #19328.

- **Replication:** `PURGE BINARY LOGS TO` and `PURGE BINARY LOGS BEFORE` did not handle missing binary log files correctly or in the same way. Now for both of these statements, if any files listed in the `.index` file are missing from the file system, the statement fails with an error. (Bug #18199, Bug #18453)
- **Replication:** `START SLAVE UNTIL MASTER_LOG_POS=position` issued on a slave that was using `--log-slave-updates` and that was involved in circular replication would cause the slave to run and stop one event later than that specified by the value of `position`. (Bug #13861)
- On Windows, the installer attempted to use JScript to determine whether the target data directory already existed. On Windows Vista x64, this resulted in an error because the installer was attempting to run the JScript in a 32-bit engine, which wasn't registered on Vista. The installer no longer uses JScript but instead relies on a native WiX command. (Bug #36103)
- There was a memory leak when connecting to a `FEDERATED` table using a connection string that had a host value of `localhost` or omitted the host and a port value of `0` or omitted the port. (Bug #35509)

- Using `LOAD DATA INFILE` with a view could crash the server. (Bug #35469)
- When a view containing a reference to `DUAL` was created, the reference was removed when the definition was stored, causing some queries against the view to fail with invalid SQL syntax errors. (Bug #35193)
- Debugging symbols were missing for some executables in Windows binary distributions. (Bug #35104)
- A query that performed a `ref_or_null` join where the second table used a key having one or columns that could be `NULL` and had a column value that was `NULL` caused the server to crash. (Bug #34945)

References: This issue is a regression of: Bug #12144.

- Some binaries produced stack corruption messages due to being built with versions of `bison` older than 2.1. Builds are now created using `bison` 2.3. (Bug #34926)
- `mysqldump` failed to return an error code when using the `--master-data` option without binary logging being enabled on the server. (Bug #34909)
- Under some circumstances, the value of `mysql_insert_id()` following a `SELECT ... INSERT` statement could return an incorrect value. This could happen when the last `SELECT ... INSERT` did not involve an `AUTO_INCREMENT` column, but the value of `mysql_insert_id()` was changed by some previous statements. (Bug #34889)
- Table and database names were mixed up in some places of the subquery transformation procedure. This could affect debugging trace output and further extensions of that procedure. (Bug #34830)
- A malformed URL used for a `FEDERATED` table's `CONNECTION` option value in a `CREATE TABLE` statement was not handled correctly and could crash the server. (Bug #34788)
- Queries such as `SELECT ROW(1, 2) IN (SELECT t1.a, 2) FROM t1 GROUP BY t1.a` (combining row constructors and subqueries in the `FROM` clause) could lead to assertion failure or unexpected error messages. (Bug #34763)
- Using `NAME_CONST()` with a negative number and an aggregate function caused MySQL to crash. This could also have a negative impact on replication. (Bug #34749)
- A memory-handling error associated with use of `GROUP_CONCAT()` in subqueries could result in a server crash. (Bug #34747)
- For an indexed integer column `col_name` and a value `N` that is one greater than the maximum value permitted for the data type of `col_name`, conditions of the form `WHERE col_name < N` failed to return rows where the value of `col_name` is `N - 1`. (Bug #34731)
- Executing a `TRUNCATE TABLE` statement on a table having both a foreign key reference and a `DELETE` trigger crashed the server. (Bug #34643)
- Some subqueries using an expression that included an aggregate function could fail or in some cases lead to a crash of the server. (Bug #34620)
- A server crash could occur if `INFORMATION_SCHEMA` tables built in memory were swapped out to disk during query execution. (Bug #34529)
- `CAST(AVG(arg) AS DECIMAL)` produced incorrect results for non-`DECIMAL` arguments. (Bug #34512)
- Under some conditions, a `SET GLOBAL innodb_commit_concurrency` or `SET GLOBAL innodb_autoextend_increment` statement could fail. (Bug #34223)

References: This issue is a regression of: Bug #31177.

- `mysqldump` attempts to set the `character_set_results` system variable after connecting to the server. This failed for pre-4.1 servers that have no such variable, but `mysqldump` did not account for this and 1) failed to dump database contents; 2) failed to produce any error message alerting the user to the problem. (Bug #34192)
- For a `FEDERATED` table with an index on a nullable column, accessing the table could crash a server, return an incorrect result set, or return `ERROR 1030 (HY000): Got error 1430 from storage engine`. (Bug #33946)
- A query using `WHERE (column1='string1' AND column2=constant1) OR (column1='string2' AND column2=constant2)`, where `col1` used a binary collation and `string1` matched `string2` except for case, failed to match any records even when matches were found by a query using the equivalent clause `WHERE column2=constant1 OR column2=constant2`. (Bug #33833)
- Reuse of prepared statements could cause a memory leak in the embedded server. (Bug #33796)
- Some queries using a combination of `IN`, `CONCAT()`, and an implicit type conversion could return an incorrect result. (Bug #33764)
- In some cases a query that produced a result set when using `ORDER BY ASC` did not return any results when this was changed to `ORDER BY DESC`. (Bug #33758)
- Disabling concurrent inserts caused some cacheable queries not to be saved in the query cache. (Bug #33756)
- Certain combinations of views, subselects with outer references and stored routines or triggers could cause the server to crash. (Bug #33389)
- `SLEEP(0)` failed to return on 64-bit Mac OS X due to a bug in `pthread_cond_timedwait()`. (Bug #33304)
- Granting the `UPDATE` privilege on one column of a view caused the server to crash. (Bug #33201)
- Under some circumstances a combination of aggregate functions and `GROUP BY` in a `SELECT` query over a view could lead to incorrect calculation of the result type of the aggregate function. This in turn could lead to incorrect results, or to crashes on debug builds of the server. (Bug #33049)
- For `DISTINCT` queries, MySQL 4.0 and 4.1 stopped reading joined tables as soon as the first matching row was found. However, this optimization was lost in MySQL 5.0, which instead read all matching rows. This fix for this regression may result in a major improvement in performance for `DISTINCT` queries in cases where many rows match. (Bug #32942)
- Incorrect assertions could cause a server crash for `DELETE` triggers for transactional tables. (Bug #32790)
- Inserting strings with a common prefix into a table that used the `ucs2` character set corrupted the table. (Bug #32705)
- Queries using `LIKE` on tables having indexed `CHAR` columns using either of the `eucjpm`s or `ujis` character sets did not return correct results. (Bug #32510)
- Queries testing numeric constants containing leading zeros against `ZEROFILL` columns were not evaluated correctly. (Bug #31887)
- If an error occurred during file creation, the server sometimes did not remove the file, resulting in an unused file in the file system. (Bug #31781)

- The server returned the error message `Out of memory; restart server and try again` when the actual problem was that the sort buffer was too small. Now an appropriate error message is returned in such cases. (Bug #31590)
- A data file required for the `ndb_restore_different_endian_data` test case was missing from binary distributions, causing the test to fail. The data file now is included. (Bug #31453, Bug #11747239)
- When sorting privilege table rows, the server treated escaped wildcard characters (`\%` and `_`) the same as unescaped wildcard characters (`%` and `_`), resulting in incorrect row ordering. (Bug #31194)
- On Windows, `SHOW PROCESSLIST` could display process entries with a `State` value of `*** DEAD ***`. (Bug #30960)
- If an alias was used to refer to the value returned by a stored function within a subselect, the outer select recognized the alias but failed to retrieve the value assigned to it in the subselect. (Bug #30787)

References: This issue is a regression of: Bug #20777.

- Binary logging for a stored procedure differed depending on whether or not execution occurred in a prepared statement. (Bug #30604)
- An orphaned PID file from a no-longer-running process could cause `mysql.server` to wait for that process to exit even though it does not exist. (Bug #30378)
- The `mysql_config` command would output `CFLAGS` values that were incompatible with C++ for the HP-UX platform. (Bug #29645)
- The SQL parser did not accept an empty `UNION=()` clause. This meant that, when there were no underlying tables specified for a `MERGE` table, `SHOW CREATE TABLE` and `mysqldump` both output statements that could not be executed.

Now it is possible to execute a `CREATE TABLE` or `ALTER TABLE` statement with an empty `UNION=()` clause. However, `SHOW CREATE TABLE` and `mysqldump` do not output the `UNION=()` clause if there are no underlying tables specified for a `MERGE` table. This also means it is now possible to remove the underlying tables for a `MERGE` table using `ALTER TABLE ... UNION=()`. (Bug #28248)

- It was possible to exhaust memory by repeatedly running `index_merge` queries and never performing any `FLUSH TABLES` statements. (Bug #27732)
- When `utf8` was set as the connection character set, using `SPACE()` with a non-Unicode column produced an error. (Bug #27580)

References: See also: Bug #23637.

- In `ORDER BY` clauses, mixing aggregate functions and nongrouping columns is not permitted if the `ONLY_FULL_GROUP_BY` SQL mode is enabled. However, in some cases, no error was thrown because of insufficient checking. (Bug #27219)
- For the `--record_log_pos` option, `mysqlhotcopy` now determines the slave status information from the result of `SHOW SLAVE STATUS` by using the `Relay_Master_Log_File` and `Exec_Master_Log_Pos` values rather than the `Master_Log_File` and `Read_Master_Log_Pos` values. This provides a more accurate indication of slave execution relative to the master. (Bug #27101)
- The MySQL Instance Configuration Wizard would not permit you to choose a service name, even though the criteria for the service name were valid. The code that checks the name has been updated to support the correct criteria of any string less than 256 character and not containing either a forward or backward slash character. (Bug #27013)

- `config-win.h` unconditionally defined `bool` as `BOOL`, causing problems on systems where `bool` is 1 byte and `BOOL` is 4 bytes. (Bug #26461)
- On Windows, for distributions built with debugging support, `mysql` could crash if the user typed **Control +C**. (Bug #26243)
- On Windows, an error in `configure.js` caused installation of source distributions to fail. (Bug #25340)
- Using `mysqldump` in MySQL 5.1 resulted in dump files that could not be loaded in MySQL 5.0 because `USING type_name` options in index definitions appeared after the index column list, whereas 5.0 accepted only the old syntax that has `USING` before the column list. The parser in 5.0 now accepts `USING` following the column list. (Bug #25162)
- The client library had no way to return an error if no connection had been established. This caused problems such as `mysql_library_init()` failing silently if no `errmsg.sys` file was available. (Bug #25097)
- On Mac OS X, the StartupItem for MySQL did not work. (Bug #25008)
- For Windows 64-bit builds, enabling shared-memory support caused client connections to fail. (Bug #24992)
- If a user installed MySQL Server and set a password for the `root` user, and then uninstalled and reinstalled MySQL Server to the same location, the user could not use the MySQL Instance Config wizard to configure the server because the uninstall operation left the previous data directory intact. The config wizard *assumed* that any new install (not an upgrade) would have the default data directory where the `root` user has no password. The installer now writes a registry key named `FoundExistingDataDir`. If the installer finds an existing data directory, the key will have a value of 1, otherwise it will have a value of 0. When `MySQLInstanceConfig.exe` is run, it will attempt to read the key. If it can read the key, and the value is 1 and there is no existing instance of the server (indicating a new installation), the Config Wizard will permit the user to input the old password so the server can be configured. (Bug #24215)
- The MySQL header files contained some duplicate macro definitions that could cause compilation problems. (Bug #23839)
- `SHOW COLUMNS` on a `TEMPORARY` table caused locking issues. (Bug #23588)
- For distributions compiled with the bundled `libedit` library, there were difficulties using the `mysql` client to enter input for non-ASCII or multibyte characters. (Bug #23097)
- On Mac OS X, `mysqld` did not react to Control+C when run under `gdb`, even when run with the `--gdb` option. (Bug #21567)
- `mysql-stress-test.pl` and `mysqld_multi.server.sh` were missing from some binary distributions. (Bug #21023, Bug #25486)
- A `SET` column whose definition specified 64 elements could not be updated using integer values. (Bug #15409)
- `MySQLInstanceConfig.exe` did not save the `innodb_data_home_dir` value to the `my.ini` file under certain circumstances. (Bug #6627)

Changes in MySQL Enterprise 5.0.58 [MRU] (2008-03-05)

This is a *Monthly Rapid Update* release of the MySQL Enterprise Server 5.0.

This section documents all changes and bugfixes that have been applied since the last MySQL Enterprise Server release (5.0.56). If you would like to receive more fine-grained and personalized *update alerts* about fixes that are relevant to the version and features you use, please consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details please see <http://www.mysql.com/products/enterprise/advisors.html>.

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- **Important Change; Cluster API:** Because `NDB_LE_MemoryUsage.page_size_kb` shows memory page sizes in bytes rather than kilobytes, it has been renamed to `page_size_bytes`. The name `page_size_kb` is now deprecated and thus subject to removal in a future release, although it currently remains supported for reasons of backward compatibility. See [The Ndb_logevent_type Type](#), for more information about `NDB_LE_MemoryUsage`. (Bug #30271)
- The `ndbd` and `ndb_mgmd` man pages have been reclassified from volume 1 to volume 8. (Bug #34642)
- `mysqltest` now has `mkdir` and `rmdir` commands for creating and removing directories. (Bug #31004)

Bugs Fixed

- **Performance:** `InnoDB` adaptive hash latches could be held too long during filesort operations, resulting in a server crash. Now the hash latch is released when a query on `InnoDB` tables performs a filesort. This eliminates the crash and may provide significant performance improvements on systems on which many queries using filesorts with temporary tables are being performed. (Bug #32149)
- **MySQL Cluster:** When configured with `NDB` support, MySQL failed to compile using `gcc` 4.3 on 64bit FreeBSD systems. (Bug #34169)
- **MySQL Cluster:** The failure of a DDL statement could sometimes lead to node failures when attempting to execute subsequent DDL statements. (Bug #34160)
- **MySQL Cluster:** Extremely long `SELECT` statements (where the text of the statement was in excess of 50000 characters) against `NDB` tables returned empty results. (Bug #34107)
- **MySQL Cluster:** A periodic failure to flush the send buffer by the `NDB` TCP transporter could cause a unnecessary delay of 10 ms between operations. (Bug #34005)
- **MySQL Cluster:** When all data and SQL nodes in the cluster were shut down abnormally (that is, other than by using `STOP` in the cluster management client), `ndb_mgm` used excessive amounts of CPU. (Bug #33237)
- **MySQL Cluster:** Transaction atomicity was sometimes not preserved between reads and inserts under high loads. (Bug #31477)
- **MySQL Cluster:** Numerous `NDBCLUSTER` test failures occurred in builds compiled using `icc` on IA64 platforms. (Bug #31239)
- **MySQL Cluster:** Having tables with a great many columns could cause Cluster backups to fail. (Bug #30172)
- **MySQL Cluster:** Issuing an `INSERT ... ON DUPLICATE KEY UPDATE` concurrently with or following a `TRUNCATE TABLE` statement on an `NDB` table failed with `NDB` error 4350 `Transaction already aborted`. (Bug #29851)

- **MySQL Cluster:** It was possible in `config.ini` to define cluster nodes having node IDs greater than the maximum permitted value. (Bug #28298)
- **Cluster API:** When reading a `BIT(64)` value using `NdbOperation::getValue()`, 12 bytes were written to the buffer rather than the expected 8 bytes. (Bug #33750)
- `mysql_explain_log` concatenated multiple-line statements, causing malformed results for statements that contained SQL comments beginning with `--`. (Bug #34339)
- Executing an `ALTER VIEW` statement on a table crashed the server. (Bug #34337)
- Passing anything other than an integer argument to a `LIMIT` clause in a prepared statement would fail. (This limitation was introduced to avoid replication problems; for example, replicating the statement with a string argument would cause a parse failure in the slave). Now, arguments to the `LIMIT` clause are converted to integer values, and these converted values are used when logging the statement. (Bug #33851)
- An internal buffer in `mysql` was too short. Overextending it could cause stack problems or segmentation violations on some architectures. (This is not a problem that could be exploited to run arbitrary code.) (Bug #33841)
- Large unsigned integers were improperly handled for prepared statements, resulting in truncation or conversion to negative numbers. (Bug #33798)
- `make_binary_distribution` passed the `--print-libgcc-file` option to the C compiler, but this does not work with the `ICC` compiler. (Bug #33536)
- When MySQL was built with OpenSSL, the SSL library was not properly initialized with information of which endpoint it was (server or client), causing connection failures. (Bug #33050)
- Repeated creation and deletion of views within prepared statements could eventually crash the server. (Bug #32890)

References: See also: Bug #34587.

- Executing a prepared statement associated with a materialized cursor sent to the client a metadata packet with incorrect table and database names. The problem occurred because the server sent the name of the temporary table used by the cursor instead of the table name of the original table.

The same problem occurred when selecting from a view, in which case the name of the table name was sent, rather than the name of the view. (Bug #32265)

- `SHOW STATUS` caused a server crash if `InnoDB` had not been initialized. (Bug #32083)
- The `mysqld` crash handler failed on Windows. (Bug #31745)
- The MySQL preferences pane did not work to start or stop MySQL on Mac OS X 10.5 (Leopard). (Bug #28854)
- For upgrading to a new major version using RPM packages (such as 4.1 to 5.0), if the installation procedure found an existing MySQL server running, it could fail to shut down the old server, but also erroneously removed the server's socket file. Now the procedure checks for an existing server package from a different vendor or major MySQL version. In such case, it refuses to install the server and recommends how to safely remove the old packages before installing the new ones. (Bug #28555)
- `mysqlhotcopy` silently skipped databases with names consisting of two alphanumeric characters. (Bug #28460)

- `mysql` did not use its completion table. Also, the table contained few entries. (Bug #24624)
- `mysql_config` output did not include `-lmygcc` on some platforms when it was needed. (Bug #21158)

Changes in MySQL Enterprise 5.0.56sp1 [QSP] (2008-03-30)

This is a *Service Pack* release of the MySQL Enterprise Server 5.0.

This section documents all changes and bugfixes that have been applied in MySQL 5.0.56sp1 since the previous MySQL Enterprise Server Quarterly Service Pack release (5.0.50sp1a). If you would like to receive more fine-grained and personalized *update alerts* about fixes that are relevant to the version and features you use, please consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details please see <http://www.mysql.com/products/enterprise/advisors.html>.

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- `mysqldump` produces a `-- Dump completed on DATE` comment at the end of the dump if `-- comments` is given. The date causes dump files for identical data take at different times to appear to be different. The new options `--dump-date` and `--skip-dump-date` control whether the date is added to the comment. `--skip-dump-date` suppresses date printing. The default is `--dump-date` (include the date in the comment). (Bug #31077)
- The `mysql_odbc_escape_string()` C API function has been removed. It has multibyte character escaping issues, doesn't honor the `NO_BACKSLASH_ESCAPES` SQL mode and is not needed anymore by Connector/ODBC as of 3.51.17. (Bug #29592)

References: See also: Bug #41728.

- The default value of the `connect_timeout` system variable was increased from 5 to 10 seconds. This might help in cases where clients frequently encounter errors of the form `Lost connection to MySQL server at 'XXX', system error: errno`. (Bug #28359)
- The use of InnoDB hash indexes now can be controlled by setting the new `innodb_adaptive_hash_index` system variable at server startup. By default, this variable is enabled. See [Adaptive Hash Indexes](#).
- The argument for the `mysql-test-run.pl --do-test` and `--skip-test` options is now interpreted as a Perl regular expression if there is a pattern metacharacter in the argument value. This enables more flexible specification of which tests to perform or skip.

Bugs Fixed

- **Security Fix:** Using `RENAME TABLE` against a table with explicit `DATA DIRECTORY` and `INDEX DIRECTORY` options can be used to overwrite system table information by replacing the symbolic link points. the file to which the symlink points.

MySQL will now return an error when the file to which the symlink points already exists. (Bug #32111, CVE-2007-5969)

- **Security Fix:** `ALTER VIEW` retained the original `DEFINER` value, even when altered by another user, which could enable that user to gain the access rights of the view. Now `ALTER VIEW` is permitted only to the original definer or users with the `SUPER` privilege. (Bug #29908)

- **Security Fix:** When using a [FEDERATED](#) table, the local server could be forced to crash if the remote server returned a result with fewer columns than expected. (Bug #29801)
- **Security Enhancement:** It was possible to force an error message of excessive length which could lead to a buffer overflow. This has been made no longer possible as a security precaution. (Bug #32707)
- **Performance:** [InnoDB](#) had a race condition for an adaptive hash rw-lock waiting for an X-lock. This fix may also provide significant speed improvements on systems experiencing problems with contention for the adaptive hash index. (Bug #29560)
- **Incompatible Change:** With [ONLY_FULL_GROUP_BY](#) SQL mode enabled, queries such as `SELECT a FROM t1 HAVING COUNT(*)>2` were not being rejected as they should have been.

This fix results in the following behavior:

- There is a check against mixing group and nongroup columns *only* when [ONLY_FULL_GROUP_BY](#) is enabled.
- This check is done both for the select list and for the [HAVING](#) clause if there is one.

This behavior differs from previous versions as follows:

- Previously, the [HAVING](#) clause was not checked when [ONLY_FULL_GROUP_BY](#) was enabled; now it is checked.
- Previously, the select list was checked even when [ONLY_FULL_GROUP_BY](#) was not enabled; now it is checked only when [ONLY_FULL_GROUP_BY](#) is enabled.

(Bug #31794)

- **Incompatible Change:** The MySQL 5.0.50 patch for this bug was reverted because it changed the behavior of a General Availability MySQL release. (Bug #30234)

References: See also: Bug #27525.

- **Incompatible Change:** It was possible to create a view having a column whose name consisted of an empty string or space characters only.

One result of this bug fix is that aliases for columns in the view [SELECT](#) statement are checked to ensure that they are legal column names. In particular, the length must be within the maximum column length of 64 characters, not the maximum alias length of 256 characters. This can cause problems for replication or loading dump files. For additional information and workarounds, see [Restrictions on Views](#). (Bug #27695)

References: See also: Bug #31202.

- **Incompatible Change:** Several type-preserving functions and operators returned an incorrect result type that does not match their argument types: [COALESCE\(\)](#), [IF\(\)](#), [IFNULL\(\)](#), [LEAST\(\)](#), [GREATEST\(\)](#), [CASE](#). These now aggregate using the precise SQL types of their arguments rather than the internal type. In addition, the result type of the [STR_TO_DATE\(\)](#) function is now [DATETIME](#) by default. (Bug #27216)
- **Incompatible Change:** It was possible for option files to be read twice at program startup, if some of the standard option file locations turned out to be the same directory. Now duplicates are removed from the list of files to be read.

Also, users could not override system-wide settings using `~/my.cnf` because `SYSCONFDIR/my.cnf` was read last. The latter file now is read earlier so that `~/my.cnf` can override system-wide settings.

The fix for this problem had a side effect such that on Unix, MySQL programs looked for options in `~/my.cnf` rather than the standard location of `~/my.cnf`. That problem is addressed in Bug #38180. (Bug #20748)

References: See also: Bug #38180.

- **Important Change; MySQL Cluster:** `AUTO_INCREMENT` columns had the following problems when used in `NDB` tables:
 - The `AUTO_INCREMENT` counter was not updated correctly when such a column was updated.
 - `AUTO_INCREMENT` values were not prefetched beyond statement boundaries.
 - `AUTO_INCREMENT` values were not handled correctly with `INSERT IGNORE` statements.
 - After being set, `ndb_autoincrement_prefetch_sz` showed a value of 1, regardless of the value it had actually been set to.As part of this fix, the behavior of `ndb_autoincrement_prefetch_sz` has changed. Setting this to less than 32 no longer has any effect on prefetching within statements (where IDs are now always obtained in batches of 32 or more), but only between statements. The default value for this variable has also changed, and is now 1. (Bug #25176, Bug #31956, Bug #32055)
- **Important Change; Replication:** When the master crashed during an update on a transactional table while in `autocommit` mode, the slave failed. This fix causes every transaction (including `autocommit` transactions) to be recorded in the binary log as starting with a `BEGIN` and ending with a `COMMIT` or `ROLLBACK`.

**Note**

The current fix does *not* cause nontransactional changes to be wrapped in `BEGIN ... COMMIT` or `BEGIN ... ROLLBACK` when written to the binary log. For this purpose, any statements affecting tables using a nontransactional storage engine such as `MyISAM` are regarded as nontransactional, even when `autocommit` is enabled.

(Bug #26395)

References: See also: Bug #29288, Bug #49522.

- **Important Note; Replication:** Network timeouts between the master and the slave could result in corruption of the relay log. This fix rectifies a long-standing replication issue when using unreliable networks, including replication over wide area networks such as the Internet. If you experience reliability issues and see many `You have an error in your SQL syntax` errors on replication slaves, we strongly recommend that you upgrade to a MySQL version which includes this fix. (Bug #26489)
- **MySQL Cluster:** An improperly reset internal signal was observed as a hang when using events in the `NDB` API but could result in various errors. (Bug #33206)
- **MySQL Cluster:** Incorrectly handled parameters could lead to a crash in the Transaction Coordinator during a node failure, causing other data nodes to fail. (Bug #33168)
- **MySQL Cluster:** The failure of a master node could lead to subsequent failures in local checkpointing. (Bug #32160)
- **MySQL Cluster:** An uninitialized variable in the `NDB` storage engine code led to `AUTO_INCREMENT` failures when the server was compiled with `gcc 4.2.1`. (Bug #31848)

References: This issue is a regression of: Bug #27437.

- **MySQL Cluster:** An error with an `if` statement in `sql/ha_ndbcluster.cc` could potentially lead to an infinite loop in case of failure when working with `AUTO_INCREMENT` columns in `NDB` tables. (Bug #31810)
- **MySQL Cluster:** The `NDB` storage engine code was not safe for strict-alias optimization in `gcc` 4.2.1. (Bug #31761)
- **MySQL Cluster:** Primary keys on variable-length columns (such as `VARCHAR`) did not work correctly. (Bug #31635)
- **MySQL Cluster:** Transaction timeouts were not handled well in some circumstances, leading to excessive number of transactions being aborted unnecessarily. (Bug #30379)
- **MySQL Cluster:** In some cases, the cluster management server logged entries multiple times following a restart of `ndb_mgmd`. (Bug #29565)
- **MySQL Cluster:** An interpreted program of sufficient size and complexity could cause all cluster data nodes to shut down due to buffer overruns. (Bug #29390)
- **MySQL Cluster:** `UPDATE IGNORE` could sometimes fail on `NDB` tables due to the use of uninitialized data when checking for duplicate keys to be ignored. (Bug #25817)
- **MySQL Cluster:** When inserting a row into an `NDB` table with a duplicate value for a nonprimary unique key, the error issued would reference the wrong key.

This improves on an initial fix for this issue made in MySQL 5.0.30 and MySQL 5.0.33 (Bug #21072)

- **Replication:** A `CREATE USER`, `DROP USER`, or `RENAME USER` statement that fails on the master, or that is a duplicate of any of these statements, is no longer written to the binary log; previously, either of these occurrences could cause the slave to fail. (Bug #33862)

References: See also: Bug #29749.

- **Replication:** `SHOW BINLOG EVENTS` could fail when the binary log contained one or more events whose size was close to the value of `max_allowed_packet`. (Bug #33413)
- **Replication:** SQL statements containing comments using `--` syntax were not replayable by `mysqlbinlog`, even though such statements replicated correctly. (Bug #32205)
- **Replication:** It was possible for the name of the relay log file to exceed the amount of memory reserved for it, possibly leading to a crash of the server. (Bug #31836)

References: See also: Bug #28597.

- **Replication:** Corruption of log events caused the server to crash on 64-bit Linux systems having 4 GB or more of memory. (Bug #31793)
- **Replication:** Use of the `@hostname` system variable in inserts in `mysql_system_tables_data.sql` did not replicate. The workaround is to select its value into a user variable (which does replicate) and insert that. (Bug #31167)
- **Replication:** Issuing a `DROP VIEW` statement caused replication to fail if the view did not actually exist. (Bug #30998)
- **Replication:** One thread could read uninitialized memory from the stack of another thread. This issue was only known to occur in a `mysqld` process acting as both a master and a slave. (Bug #30752)

- **Replication:** Replication of `LOAD DATA INFILE` could fail when `read_buffer_size` was larger than `max_allowed_packet`. (Bug #30435)
- **Replication:** Setting `server_id` did not update its value for the current session. (Bug #28908)
- **Replication:** Due a previous change in how the default name and location of the binary log file were determined, replication failed following some upgrades. (Bug #28597, Bug #28603)

References: See also: Bug #31836. This issue is a regression of: Bug #20166.

- **Replication:** Stored procedures having `BIT` parameters were not replicated correctly. (Bug #26199)
- **Replication:** Issuing `SHOW SLAVE STATUS` as `mysqld` was shutting down could cause a crash. (Bug #26000)
- **Replication:** An `UPDATE` statement using a stored function that modified a nontransactional table was not logged if it failed. This caused the copy of the nontransactional table on the master have a row that the copy on the slave did not.

In addition, when an `INSERT ... ON DUPLICATE KEY UPDATE` statement encountered a duplicate key constraint, but the `UPDATE` did not actually change any data, the statement was not logged. As a result of this fix, such statements are now treated the same for logging purposes as other `UPDATE` statements, and so are written to the binary log. (Bug #23333)

References: See also: Bug #12713.

- **Replication:** A replication slave sometimes failed to reconnect because it was unable to run `SHOW SLAVE HOSTS`. It was not necessary to run this statement on slaves (since the master should track connection IDs), and the execution of this statement by slaves was removed. (Bug #21132)

References: See also: Bug #13963, Bug #21869.

- The server crashed when executing a query that had a subquery containing an equality `X=Y` where `Y` referred to a named select list expression from the parent select. The server crashed when trying to use the `X=Y` equality for `ref`-based access. (Bug #33794)
- Use of uninitialized memory for `filesort` in a subquery caused a server crash. (Bug #33675)
- The server could crash when `REPEAT` or another control instruction was used in conjunction with labels and a `LEAVE` instruction. (Bug #33618)
- The parser permitted control structures in compound statements to have mismatched beginning and ending labels. (Bug #33618)
- `SET GLOBAL myisam_max_sort_file_size=DEFAULT` set `myisam_max_sort_file_size` to an incorrect value. (Bug #33382)

References: See also: Bug #31177.

- `CREATE TABLE ... SELECT` created tables that for date columns used the obsolete `Field_date` type instead of `Field_newdate`. (Bug #33256)
- For `DECIMAL` columns used with the `ROUND(X,D)` or `TRUNCATE(X,D)` function with a nonconstant value of `D`, adding an `ORDER BY` for the function result produced misordered output. (Bug #33143)

References: See also: Bug #33402, Bug #30617.

- Some valid `SELECT` statements could not be used as views due to incorrect column reference resolution. (Bug #33133)

- The fix for Bug #11230 and Bug #26215 introduced a significant input-parsing slowdown for the `mysql` client. This has been corrected. (Bug #33057)

References: See also: Bug #11230, Bug #26215.

- `UNION` constructs cannot contain `SELECT ... INTO` except in the final `SELECT`. However, if a `UNION` was used in a subquery and an `INTO` clause appeared in the top-level query, the parser interpreted it as having appeared in the `UNION` and raised an error. (Bug #32858)
- The correct data type for a `NULL` column resulting from a `UNION` could be determined incorrectly in some cases: 1) Not correctly inferred as `NULL` depending on the number of selects; 2) Not inferred correctly as `NULL` if one select used a subquery. (Bug #32848)
- An `ORDER BY` query using `IS NULL` in the `WHERE` clause did not return correct results. (Bug #32815)
- For queries containing `GROUP_CONCAT(DISTINCT col_list ORDER BY col_list)`, there was a limitation that the `DISTINCT` columns had to be the same as `ORDER BY` columns. Incorrect results could be returned if this was not true. (Bug #32798)
- The `LAST_DAY()` function returns a `DATE` value, but internally the value did not have the time fields zeroed and calculations involving the value could return incorrect results. (Bug #32770)
- Use of the `cp932` character set with `CAST()` in an `ORDER BY` clause could cause a server crash. (Bug #32726)
- A subquery using an `IS NULL` check of a column defined as `NOT NULL` in a table used in the `FROM` clause of the outer query produced an invalid result. (Bug #32694)
- Specifying a nonexistent column for an `INSERT DELAYED` statement caused a server crash rather than producing an error. (Bug #32676)
- Use of `CLIENT_MULTI_QUERIES` caused `libmysqld` to crash. (Bug #32624)
- The `INTERVAL()` function incorrectly handled `NULL` values in the value list. (Bug #32560)
- Use of a `NULL`-returning `GROUP BY` expression in conjunction with `WITH ROLLUP` could cause a server crash. (Bug #32558)

References: See also: Bug #31095.

- A `SELECT ... GROUP BY bit_column` query failed with an assertion if the length of the `BIT` column used for the `GROUP BY` was not an integer multiple of 8. (Bug #32556)
- Using `SELECT INTO OUTFILE` with 8-bit `ENCLOSED BY` characters led to corrupted data when the data was reloaded using `LOAD DATA INFILE`. This was because `SELECT INTO OUTFILE` failed to escape the 8-bit characters. (Bug #32533)
- For `FLUSH TABLES WITH READ LOCK`, the server failed to properly detect write-locked tables when running with low-priority updates, resulting in a crash or deadlock. (Bug #32528)
- A build problem introduced in MySQL 5.0.52 was resolved: The x86 32-bit Intel `icc`-compiled server binary had unwanted dependences on Intel `icc` runtime libraries. (Bug #32514)
- The rules for valid column names were being applied differently for base tables and views. (Bug #32496)
- Sending several `KILL QUERY` statements to target a connection running `SELECT SLEEP()` could freeze the server. (Bug #32436)
- `ssl-cipher` values in option files were not being read by `libmysqlclient`. (Bug #32429)

- Repeated execution of a query containing a `CASE` expression and numerous `AND` and `OR` relations could crash the server. The root cause of the issue was determined to be that the internal `SEL_ARG` structure was not properly initialized when created. (Bug #32403)
- Referencing within a subquery an alias used in the `SELECT` list of the outer query was incorrectly permitted. (Bug #32400)
- An `ORDER BY` query on a view created using a `FEDERATED` table as a base table caused the server to crash. (Bug #32374)
- Comparison of a `BIGINT NOT NULL` column with a constant arithmetic expression that evaluated to `NULL` mistakenly caused the error `Column '...' cannot be null` (error 1048). (Bug #32335)
- Assigning a 65,536-byte string to a `TEXT` column (which can hold a maximum of 65,535 bytes) resulted in truncation without a warning. Now a truncation warning is generated. (Bug #32282)
- `MIN()` and `MAX()` could return incorrect results when an index was present if a loose index scan was used. (Bug #32268)
- Memory corruption could occur due to large index map in `Range checked for each record` status reported by `EXPLAIN SELECT`. The problem was based in an incorrectly calculated length of the buffer used to store a hexadecimal representation of an index map, which could result in buffer overrun and stack corruption under some circumstances. (Bug #32241)
- Various test program cleanups were made: 1) `mytest` and `libmysqltest` were removed. 2) `bug25714` displays an error message when invoked with incorrect arguments or the `--help` option. 3) `mysql_client_test` exits cleanly with a proper error status. (Bug #32221)
- The default grant tables on Windows contained information for host `production.mysql.com`, which should not be there. (Bug #32219)
- Under certain conditions, the presence of a `GROUP BY` clause could cause an `ORDER BY` clause to be ignored. (Bug #32202)
- For comparisons of the form `date_col OP datetime_const` (where `OP` is `=`, `<`, `>`, `<=`, or `>=`), the comparison is done using `DATETIME` values, per the fix for Bug #27590. However that fix caused any index on `date_col` not to be used and compromised performance. Now the index is used again. (Bug #32198)

References: See also: Bug #27590.

- `DATETIME` arguments specified in numeric form were treated by `DATE_ADD()` as `DATE` values. (Bug #32180)
- `InnoDB` does not support `SPATIAL` indexes, but could crash when asked to handle one. Now an error is returned. (Bug #32125)
- The server crashed on optimizations involving a join of `INT` and `MEDIUMINT` columns and a system variable in the `WHERE` clause. (Bug #32103)
- With `lower_case_table_names` set, `CREATE TABLE LIKE` was treated differently by `libmysqld` than by the nonembedded server. (Bug #32063)
- Within a subquery, `UNION` was handled differently than at the top level, which could result in incorrect results or a server crash. (Bug #32036, Bug #32051)
- User-defined functions are not loaded if the server is started with the `--skip-grant-tables` option, but the server did not properly handle this case and issued an `Out of memory` error message instead. (Bug #32020)

- `HOUR()`, `MINUTE()`, and `SECOND()` could return nonzero values for `DATE` arguments. (Bug #31990)
- A column with malformed multibyte characters could cause the full-text parser to go into an infinite loop. (Bug #31950)
- Changing the SQL mode to cause dates with “zero” parts to be considered invalid (such as `'1000-00-00'`) could result in indexed and nonindexed searches returning different results for a column that contained such dates. (Bug #31928)
- In debug builds, testing the result of an `IN` subquery against `NULL` caused an assertion failure. (Bug #31884)
- `mysql-test-run.pl` sometimes set up test scenarios in which the same port number was passed to multiple servers, causing one of them to be unable to start. (Bug #31880)
- Comparison results for `BETWEEN` were different from those for operators like `<` and `>` for `DATETIME`-like values with trailing extra characters such as `'2007-10-01 00:00:00 GMT-6'`. `BETWEEN` treated the values as `DATETIME`, whereas the other operators performed a binary-string comparison. Now they all uniformly use a `DATETIME` comparison, but generate warnings for values with trailing garbage. (Bug #31800)
- Name resolution for correlated subqueries and `HAVING` clauses failed to distinguish which of two was being performed when there was a reference to an outer aliased field. This could result in error messages about a `HAVING` clause for queries that had no such clause. (Bug #31797)
- The server could crash during `filesort` for `ORDER BY` based on expressions with `INET_NTOA()` or `OCT()` if those functions returned `NULL`. (Bug #31758)
- For a fatal error during a filesort in `find_all_keys()`, the error was returned without the necessary handler uninitialization, causing an assertion failure. (Bug #31742)
- The examined-rows count was not incremented for `const` queries. (Bug #31700)
- The `mysql_change_user()` C API function was subject to buffer overflow. (Bug #31669)
- For `SELECT ... INTO outfile`, if the `ENCLOSED BY` string is empty and the `FIELDS TERMINATED BY` string started with a special character (one of `n`, `t`, `r`, `b`, `0`, `Z`, or `N`), every occurrence of the character within field values would be duplicated. (Bug #31663)
- `SHOW COLUMNS` and `DESCRIBE` displayed `null` as the column type for a view with no valid definer. This caused `mysqldump` to produce a nonreloadable dump file for the view. (Bug #31662)
- The `mysqlbug` script did not include the correct values of `CFLAGS` and `CXXFLAGS` that were used to configure the distribution. (Bug #31644)
- `ucs2` does not work as a client character set, but attempts to use it as such were not rejected. Now `character_set_client` cannot be set to `ucs2`. This also affects statements such as `SET NAMES` and `SET CHARACTER SET`. (Bug #31615)
- A buffer used when setting variables was not dimensioned to accommodate the trailing `'\0'` byte, so a single-byte buffer overrun was possible. (Bug #31588)
- `HAVING` could treat lettercase of table aliases incorrectly if `lower_case_table_names` was enabled. (Bug #31562)
- The fix for Bug #24989 introduced a problem such that a `NULL` thread handler could be used during a rollback operation. This problem is unlikely to be seen in practice. (Bug #31517)
- Killing a `CREATE TABLE ... LIKE` statement that was waiting for a name lock caused a server crash. When the statement was killed, the server attempted to release locks that were not held. (Bug #31479)

- The length of the result from `IFNULL()` could be calculated incorrectly because the sign of the result was not taken into account. (Bug #31471)
 - Queries that used the `ref` access method or index-based subquery execution over indexes that have `DECIMAL` columns could fail with an error `Column col_name cannot be null`. (Bug #31450)
 - `SELECT 1 REGEX NULL` caused an assertion failure for debug servers. (Bug #31440)
 - Executing `RENAME` while tables were open for use with `HANDLER` statements could cause a server crash. (Bug #31409)
 - `mysql-test-run.pl` tried to create files in a directory where it could not be expected to have write permission. `mysqltest` created `.reject` files in a directory other than the one where test results go. (Bug #31398)
 - `DROP USER` caused an increase in memory usage. (Bug #31347)
 - For an almost-full `MyISAM` table, an insert that failed could leave the table in a corrupt state. (Bug #31305)
 - `myisamchk --unpack` could corrupt a table that when unpacked has static (fixed-length) row format. (Bug #31277)
 - `CONVERT(val, DATETIME)` failed on invalid input, but processing was not aborted for the `WHERE` clause, leading to a server crash. (Bug #31253)
 - Allocation of an insufficiently large group-by buffer following creation of a temporary table could lead to a server crash. (Bug #31249)
 - Use of `DECIMAL(n, n) ZEROFILL` in `GROUP_CONCAT()` could cause a server crash. (Bug #31227)
 - Server variables could not be set to their current values on Linux platforms. (Bug #31177)
- References: See also: Bug #6958.
- With small values of `myisam_sort_buffer_size`, `REPAIR TABLE` for `MyISAM` tables could cause a server crash. (Bug #31174)
 - If `MAKETIME()` returned `NULL` when used in an `ORDER BY` that was evaluated using `filesort`, a server crash could result. (Bug #31160)
 - Full-text searches on `ucs2` columns caused a server crash. (`FULLTEXT` indexes on `ucs2` columns cannot be used, but it should be possible to perform `IN BOOLEAN MODE` searches on `ucs2` columns without a crash.) (Bug #31159)
 - Data in `BLOB` or `GEOMETRY` columns could be cropped when performing a `UNION` query. (Bug #31158)
 - An assertion designed to detect a bug in the `ROLLUP` implementation would incorrectly be triggered when used in a subquery context with noncacheable statements. (Bug #31156)
 - Selecting spatial types in a `UNION` could cause a server crash. (Bug #31155)
 - Use of `GROUP_CONCAT(DISTINCT bit_column)` caused an assertion failure. (Bug #31154)
 - The server crashed in the parser when running out of memory. Memory handling in the parser has been improved to gracefully return an error when out-of-memory conditions occur in the parser. (Bug #31153)
 - MySQL declares a `UNIQUE` key as a `PRIMARY` key if it doesn't have `NULL` columns and is not a partial key, and the `PRIMARY` key must always be the first key. However, in some cases, a nonfirst key could

be reported as `PRIMARY`, leading to an assert failure by `InnoDB`. This is fixed by correcting the key sort order. (Bug #31137)

- `GROUP BY NULL WITH ROLLUP` could cause a server crash. (Bug #31095)

References: See also: Bug #32558.

- `REGEXP` operations could cause a server crash for character sets such as `ucs2`. Now the arguments are converted to `utf8` if possible, to permit correct results to be produced if the resulting strings contain only 8-bit characters. (Bug #31081)
- Internal conversion routines could fail for several multibyte character sets (`big5`, `cp932`, `euckr`, `gb2312`, `sjis`) for empty strings or during evaluation of `SOUNDS LIKE`. (Bug #31069, Bug #31070)
- Many nested subqueries in a single query could led to excessive memory consumption and possibly a crash of the server. (Bug #31048)
- The `MOD()` function and the `%` operator crashed the server for a divisor less than 1 with a very long fractional part. (Bug #31019)
- On Windows, the `pthread_mutex_trylock()` implementation was incorrect. (Bug #30992)
- A character set introducer followed by a hexadecimal or bit-value literal did not check its argument and could return an ill-formed result for invalid input. (Bug #30986)
- `CHAR(str USING charset)` did not check its argument and could return an ill-formed result for invalid input. (Bug #30982)
- The result from `CHAR(str USING ucs2)` did not add a leading 0x00 byte for input strings with an odd number of bytes. (Bug #30981)
- The `GeomFromText()` function could cause a server crash if the first argument was `NULL` or the empty string. (Bug #30955)
- `MAKEDATE()` incorrectly moved year values in the 100 to 200 range into the 1970 to 2069 range. (This is legitimate for 00 to 99, but three-digit years should be used unchanged.) (Bug #30951)
- When invoked with constant arguments, `STR_TO_DATE()` could use a cached value for the format string and return incorrect results. (Bug #30942)
- `GROUP_CONCAT()` returned `' , '` rather than an empty string when the argument column contained only empty strings. (Bug #30897)
- `ROUND(X,D)` or `TRUNCATE(X,D)` for nonconstant values of `D` could crash the server if these functions were used in an `ORDER BY` that was resolved using `filesort`. (Bug #30889)
- For `MEMORY` tables, lookups for `NULL` values in `BTREE` indexes could return incorrect results. (Bug #30885)
- Calling `NAME_CONST()` with nonconstant arguments triggered an assertion failure. Nonconstant arguments are no longer permitted. (Bug #30832)
- For a spatial column with a regular (non-`SPATIAL`) index, queries failed if the optimizer tried to use the index. (Bug #30825)
- Values for the `--tc-heuristic-recover` option incorrectly were treated as values for the `--myisam-stats-method` option. (Bug #30821)
- The optimizer incorrectly optimized conditions out of the `WHERE` clause in some queries involving subqueries and indexed columns. (Bug #30788)

- Improper calculation of `CASE` expression results could lead to value truncation. (Bug #30782)
- On Windows, the `pthread_mutex_trylock()` implementation was incorrect. One symptom was that invalidating the query cache could cause a server crash. (Bug #30768)
- A multiple-table `UPDATE` involving transactional and nontransactional tables caused an assertion failure. (Bug #30763)
- Under some circumstances, `CREATE TABLE ... SELECT` could crash the server or incorrectly report that the table row size was too large. (Bug #30736)
- Using the `MIN()` or `MAX()` function to select one part of a multi-part key could cause a crash when the function result was `NULL`. (Bug #30715)
- The optimizer could ignore `ORDER BY` in cases when the result set is ordered by `filesort`, resulting in rows being returned in incorrect order. (Bug #30666)
- `MyISAM` tables could not exceed 4294967295 ($2^{32} - 1$) rows on Windows. (Bug #30638)
- `mysql-test-run.pl` could not run `mysqld` with `root` privileges. (Bug #30630)
- For `MEMORY` tables, `DELETE` statements that remove rows based on an index read could fail to remove all matching rows. (Bug #30590)
- Using `GROUP BY` on an expression of the form `timestamp_col DIV number` caused a server crash due to incorrect calculation of number of decimals. (Bug #30587)
- The options available to the `CHECK TABLE` statement were also permitted in `OPTIMIZE TABLE` and `ANALYZE TABLE` statements, but caused corruption during their execution. These options were never supported for these statements, and an error is now raised if you try to apply these options to these statements. (Bug #30495)
- When expanding a `*` in a `USING` or `NATURAL` join, the check for table access for both tables in the join was done using only the grant information of the first table. (Bug #30468)
- When casting a string value to an integer, cases where the input string contained a decimal point and was long enough to overrun the `unsigned long long` type were not handled correctly. The position of the decimal point was not taken into account which resulted in miscalculated numbers and incorrect truncation to appropriate SQL data type limits. (Bug #30453)
- Versions of `mysqldump` from MySQL 4.1 or higher tried to use `START TRANSACTION WITH CONSISTENT SNAPSHOT` if the `--single-transaction` and `--master-data` options were given, even with servers older than 4.1 that do not support consistent snapshots. (Bug #30444)
- For `CREATE ... SELECT ... FROM`, where the resulting table contained indexes, adding `SQL_BUFFER_RESULT` to the `SELECT` part caused index corruption in the table. (Bug #30384)
- The optimizer made incorrect assumptions about the value of the `is_member` value for user-defined functions, sometimes resulting in incorrect ordering of UDF results. (Bug #30355)
- Some valid `euc-kr` characters having the second byte in the ranges `[0x41..0x5A]` and `[0x61..0x7A]` were rejected. (Bug #30315)
- Simultaneous `ALTER TABLE` statements for `BLACKHOLE` tables caused 100% CPU use due to locking problems. (Bug #30294)
- Setting certain values on a table using a spatial index could cause the server to crash. (Bug #30286)
- Tables with a `GEOMETRY` column could be marked as corrupt if you added a non-`SPATIAL` index on a `GEOMETRY` column. (Bug #30284)

- Some `INFORMATION_SCHEMA` tables are intended for internal use, but could be accessed by using `SHOW` statements. (Bug #30079)
- On some 64-bit systems, inserting the largest negative value into a `BIGINT` column resulted in incorrect data. (Bug #30069)
- Under some circumstances, a UDF initialization function could be passed incorrect argument lengths. (Bug #29804)
- Specifying the `--without-geometry` option for `configure` caused server compilation to fail. (Bug #29772)
- `configure` did not find `nss` on some Linux platforms. (Bug #29658)
- Views were treated as insertable even if some base table columns with no default value were omitted from the view definition. (This is contrary to the condition for insertability that a view must contain all columns in the base table that do not have a default value.) (Bug #29477)
- The `mysql` client program now ignores Unicode byte order mark (BOM) characters at the beginning of input files. Previously, it read them and sent them to the server, resulting in a syntax error.

Presence of a BOM does not cause `mysql` to change its default character set. To do that, invoke `mysql` with an option such as `--default-character-set=utf8`. (Bug #29323)
- For transactional tables, an error during a multiple-table `DELETE` statement did not roll back the statement. (Bug #29136)
- The `log` and `log_slow_queries` system variables were displayed by `SHOW VARIABLES` but could not be accessed in expressions as `@@log` and `@@log_slow_queries`. Also, attempting to set them with `SET` produced an incorrect `Unknown system variable` message. Now these variables can be accessed in expressions and attempting to set their values produces an error message that the variable is read only. (Bug #29131)
- Denormalized double-precision numbers cannot be handled properly by old MIPS processors. For IRIX, this is now handled by enabling a mode to use a software workaround. (Bug #29085)
- `SHOW VARIABLES` did not display the `relay_log`, `relay_log_index`, or `relay_log_info_file` system variables. (Bug #28893)
- When doing a `DELETE` on a table that involved a `JOIN` with `MyISAM` or `MERGE` tables and the `JOIN` referred to the same table, the operation could fail reporting `ERROR 1030 (HY000): Got error 134 from storage engine`. This was because scans on the table contents would change because of rows that had already been deleted. (Bug #28837)
- On Windows, `mysql_upgrade` created temporary files in `C:\` and did not clean them up. (Bug #28774)
- Index hints specified in view definitions were ignored when using the view to select from the base table. (Bug #28702)
- Views do not have indexes, so index hints do not apply. Use of index hints when selecting from a view is no longer permitted. (Bug #28701)
- After changing the SQL mode to a restrictive value that would make already inserted dates in a column be considered invalid, searches returned different results depending on whether the column was indexed. (Bug #28687)
- The result from `CHAR()` was incorrectly assumed in some contexts to return a single-byte result. (Bug #28550)

- The parser confused user-defined function (UDF) and stored function creation for `CREATE FUNCTION` and required that there be a default database when creating UDFs, although there is no such requirement. (Bug #28318, Bug #29816)
- The result of a comparison between `VARBINARY` and `BINARY` columns differed depending on whether the `VARBINARY` column was indexed. (Bug #28076)
- The metadata in some `MYSQL_FIELD` members could be incorrect when a temporary table was used to evaluate a query. (Bug #27990)
- An `ORDER BY` at the end of a `UNION` affected individual `SELECT` statements rather than the overall query result. (Bug #27848)
- `comp_err` created files with permissions such that they might be inaccessible during `make install` operations. (Bug #27789)
- The anonymous accounts were not being created during MySQL installation. (Bug #27692)
- A race condition between killing a statement and the thread executing the statement could lead to a situation such that the binary log contained an event indicating that the statement was killed, whereas the statement actually executed to completion. (Bug #27571)
- Some queries using the `NAME_CONST()` function failed to return either a result or an error to the client, causing it to hang. This was due to the fact that there was no check to insure that both arguments to this function were constant expressions. (Bug #27545, Bug #32559)
- With the `read_only` system variable enabled, `CREATE DATABASE` and `DROP DATABASE` were permitted to users who did not have the `SUPER` privilege. (Bug #27440)
- `resolveip` failed to produce correct results for host names that begin with a digit. (Bug #27427)
- `mysqld` sometimes miscalculated the number of digits required when storing a floating-point number in a `CHAR` column. This caused the value to be truncated, or (when using a debug build) caused the server to crash. (Bug #26788)

References: See also: Bug #12860.

- `mysqlcheck -A -r` did not correctly identify all tables that needed repairing. (Bug #25347)
- If the expected precision of an arithmetic expression exceeded the maximum precision supported by MySQL, the precision of the result was reduced by an unpredictable or arbitrary amount, rather than to the maximum precision. In some cases, exceeding the maximum supported precision could also lead to a crash of the server. (Bug #24907)
- For Windows Vista, `MySQLInstanceConfig.exe` did not include a proper manifest enabling it to run with administrative privileges. (Bug #22563)

References: See also: Bug #24732.

- Using `FLUSH TABLES` in one connection while another connection is using `HANDLER` statements caused a server crash.

**Note**

This fix supersedes a fix made previously in MySQL 5.0.32 and reverted in MySQL 5.0.48.

(Bug #21587)

References: See also: Bug #29474.

- `mysqldumpslow` returned a confusing error message when no configuration file was found. (Bug #20455)
- Host names sometimes were treated as case sensitive in account-management statements (`CREATE USER`, `GRANT`, `REVOKE`, and so forth). (Bug #19828)
- The `readline` library has been updated to version 5.2. This addresses issues in the `mysql` client where history and editing within the client failed to work as expected. (Bug #18431)
- The `Aborted_clients` status variable was incremented twice if a client exited without calling `mysql_close()`. (Bug #16918)
- Clients were ignoring the TCP/IP port number specified as the default port using the `--with-tcp-port` configuration option. (Bug #15327)
- Zero-padding of exponent values was not the same across platforms. (Bug #12860)
- Values of types `REAL ZEROFILL`, `DOUBLE ZEROFILL`, `FLOAT ZEROFILL`, were not zero-filled when converted to a character representation in the C prepared statement API. (Bug #11589)
- `mysql` stripped comments from statements sent to the server. Now the `--comments` or `--skip-comments` option can be used to control whether to retain or strip comments. The default is `--skip-comments`. (Bug #11230, Bug #26215)
- If an `INSERT ... SELECT` statement is executed, and no automatically generated value is successfully inserted, then `mysql_insert_id()` returns the ID of the last inserted row.

If no automatically generated value is successfully inserted, then `mysql_insert_id()` returns 0. (Bug #9481)

- Several buffer-size system variables were either being handled incorrectly for large values (for settings larger than 4GB, they were truncated to values less than 4GB without a warning), or were limited unnecessarily to 4GB even on 64-bit systems. The following changes were made:
 - For `key_buffer_size`, values larger than 4GB are permitted on 64-bit platforms (except Windows, for which large values are truncated to 4GB with a warning).
 - For `join_buffer_size`, `sort_buffer_size`, and `myisam_sort_buffer_size`, values are limited to 4GB on all platforms. Larger values are truncated to 4GB with a warning.

In addition, settings for `read_buffer_size` and `read_rnd_buffer_size` are limited to 2GB on all platforms. Larger values are truncated to 2GB with a warning. (Bug #5731, Bug #29419, Bug #29446)

- Executing `DISABLE KEYS` and `ENABLE KEYS` on a nonempty table would cause the size of the index file for the table to grow considerable. This was because the `DISABLE KEYS` operation would only mark the existing index, without deleting the index blocks. The `ENABLE KEYS` operation would re-create the index, adding new blocks, while the previous index blocks would remain. Existing indexes are now dropped and recreated when the `ENABLE KEYS` statement is executed. (Bug #4692)

Changes in MySQL Enterprise 5.0.56 [MRU] (2008-02-06)

This is a *Monthly Rapid Update* release of the MySQL Enterprise Server 5.0.

This section documents all changes and bugfixes that have been applied since the last MySQL Enterprise Server release (5.0.54). If you would like to receive more fine-grained and personalized *update alerts*

about fixes that are relevant to the version and features you use, please consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details please see <http://www.mysql.com/products/enterprise/advisors.html>.

Bugs Fixed

- **Important Change; MySQL Cluster:** `AUTO_INCREMENT` columns had the following problems when used in `NDB` tables:
 - The `AUTO_INCREMENT` counter was not updated correctly when such a column was updated.
 - `AUTO_INCREMENT` values were not prefetched beyond statement boundaries.
 - `AUTO_INCREMENT` values were not handled correctly with `INSERT IGNORE` statements.
 - After being set, `ndb_autoincrement_prefetch_sz` showed a value of 1, regardless of the value it had actually been set to.

As part of this fix, the behavior of `ndb_autoincrement_prefetch_sz` has changed. Setting this to less than 32 no longer has any effect on prefetching within statements (where IDs are now always obtained in batches of 32 or more), but only between statements. The default value for this variable has also changed, and is now 1. (Bug #25176, Bug #31956, Bug #32055)
- **Important Change; Replication:** When the master crashed during an update on a transactional table while in `autocommit` mode, the slave failed. This fix causes every transaction (including `autocommit` transactions) to be recorded in the binary log as starting with a `BEGIN` and ending with a `COMMIT` or `ROLLBACK`.



Note

The current fix does *not* cause nontransactional changes to be wrapped in `BEGIN ... COMMIT` or `BEGIN ... ROLLBACK` when written to the binary log. For this purpose, any statements affecting tables using a nontransactional storage engine such as `MyISAM` are regarded as nontransactional, even when `autocommit` is enabled.

(Bug #26395)

References: See also: Bug #29288, Bug #49522.

- **Important Note; Replication:** Network timeouts between the master and the slave could result in corruption of the relay log. This fix rectifies a long-standing replication issue when using unreliable networks, including replication over wide area networks such as the Internet. If you experience reliability issues and see many `You have an error in your SQL syntax` errors on replication slaves, we strongly recommend that you upgrade to a MySQL version which includes this fix. (Bug #26489)
- **MySQL Cluster:** An improperly reset internal signal was observed as a hang when using events in the `NDB` API but could result in various errors. (Bug #33206)
- **MySQL Cluster:** Incorrectly handled parameters could lead to a crash in the Transaction Coordinator during a node failure, causing other data nodes to fail. (Bug #33168)
- **MySQL Cluster:** The failure of a master node could lead to subsequent failures in local checkpointing. (Bug #32160)
- **MySQL Cluster:** Primary keys on variable-length columns (such as `VARCHAR`) did not work correctly. (Bug #31635)

- **MySQL Cluster:** When inserting a row into an `NDB` table with a duplicate value for a nonprimary unique key, the error issued would reference the wrong key.

This improves on an initial fix for this issue made in MySQL 5.0.30 and MySQL 5.0.33 (Bug #21072)

- **Replication:** A `CREATE USER`, `DROP USER`, or `RENAME USER` statement that fails on the master, or that is a duplicate of any of these statements, is no longer written to the binary log; previously, either of these occurrences could cause the slave to fail. (Bug #33862)

References: See also: Bug #29749.

- **Replication:** `SHOW BINLOG EVENTS` could fail when the binary log contained one or more events whose size was close to the value of `max_allowed_packet`. (Bug #33413)
- **Replication:** SQL statements containing comments using `--` syntax were not replayable by `mysqlbinlog`, even though such statements replicated correctly. (Bug #32205)
- **Replication:** Issuing a `DROP VIEW` statement caused replication to fail if the view did not actually exist. (Bug #30998)
- **Replication:** Replication of `LOAD DATA INFILE` could fail when `read_buffer_size` was larger than `max_allowed_packet`. (Bug #30435)
- **Replication:** Setting `server_id` did not update its value for the current session. (Bug #28908)
- The server crashed when executing a query that had a subquery containing an equality `X=Y` where `Y` referred to a named select list expression from the parent select. The server crashed when trying to use the `X=Y` equality for `ref`-based access. (Bug #33794)
- Use of uninitialized memory for `filesort` in a subquery caused a server crash. (Bug #33675)
- The server could crash when `REPEAT` or another control instruction was used in conjunction with labels and a `LEAVE` instruction. (Bug #33618)
- The parser permitted control structures in compound statements to have mismatched beginning and ending labels. (Bug #33618)
- `SET GLOBAL myisam_max_sort_file_size=DEFAULT` set `myisam_max_sort_file_size` to an incorrect value. (Bug #33382)

References: See also: Bug #31177.

- `CREATE TABLE ... SELECT` created tables that for date columns used the obsolete `Field_date` type instead of `Field_newdate`. (Bug #33256)
- For `DECIMAL` columns used with the `ROUND(X,D)` or `TRUNCATE(X,D)` function with a nonconstant value of `D`, adding an `ORDER BY` for the function result produced misordered output. (Bug #33143)

References: See also: Bug #33402, Bug #30617.

- Some valid `SELECT` statements could not be used as views due to incorrect column reference resolution. (Bug #33133)
- The fix for Bug #11230 and Bug #26215 introduced a significant input-parsing slowdown for the `mysql` client. This has been corrected. (Bug #33057)

References: See also: Bug #11230, Bug #26215.

- `UNION` constructs cannot contain `SELECT ... INTO` except in the final `SELECT`. However, if a `UNION` was used in a subquery and an `INTO` clause appeared in the top-level query, the parser interpreted it as having appeared in the `UNION` and raised an error. (Bug #32858)
- The correct data type for a `NULL` column resulting from a `UNION` could be determined incorrectly in some cases: 1) Not correctly inferred as `NULL` depending on the number of selects; 2) Not inferred correctly as `NULL` if one select used a subquery. (Bug #32848)
- For queries containing `GROUP_CONCAT(DISTINCT col_list ORDER BY col_list)`, there was a limitation that the `DISTINCT` columns had to be the same as `ORDER BY` columns. Incorrect results could be returned if this was not true. (Bug #32798)
- `HOURL()`, `MINUTE()`, and `SECOND()` could return nonzero values for `DATE` arguments. (Bug #31990)
- `mysql-test-run.pl` sometimes set up test scenarios in which the same port number was passed to multiple servers, causing one of them to be unable to start. (Bug #31880)
- Name resolution for correlated subqueries and `HAVING` clauses failed to distinguish which of two was being performed when there was a reference to an outer aliased field. This could result in error messages about a `HAVING` clause for queries that had no such clause. (Bug #31797)
- `ROUND(X,D)` or `TRUNCATE(X,D)` for nonconstant values of `D` could crash the server if these functions were used in an `ORDER BY` that was resolved using `filesort`. (Bug #30889)
- Views were treated as insertable even if some base table columns with no default value were omitted from the view definition. (This is contrary to the condition for insertability that a view must contain all columns in the base table that do not have a default value.) (Bug #29477)
- An `ORDER BY` at the end of a `UNION` affected individual `SELECT` statements rather than the overall query result. (Bug #27848)
- With the `read_only` system variable enabled, `CREATE DATABASE` and `DROP DATABASE` were permitted to users who did not have the `SUPER` privilege. (Bug #27440)
- `resolveip` failed to produce correct results for host names that begin with a digit. (Bug #27427)
- `mysqlcheck -A -r` did not correctly identify all tables that needed repairing. (Bug #25347)
- For Windows Vista, `MySQLInstanceConfig.exe` did not include a proper manifest enabling it to run with administrative privileges. (Bug #22563)

References: See also: Bug #24732.

- `mysqldumpslow` returned a confusing error message when no configuration file was found. (Bug #20455)

Changes in MySQL Enterprise 5.0.54a [MRU] (2008-01-11)

This is a *Monthly Rapid Update* release of the MySQL Enterprise Server 5.0.

This is a bugfix release that replaces MySQL 5.0.54.

Bugs Fixed

- **Security Fix:** Three vulnerabilities in yaSSL versions 1.7.5 and earlier were discovered that could lead to a server crash or execution of unauthorized code. The exploit requires a server with yaSSL enabled and TCP/IP connections enabled, but does not require valid MySQL account credentials. The exploit does not apply to OpenSSL.



Warning

The proof-of-concept exploit is freely available on the Internet. Everyone with a vulnerable MySQL configuration is advised to upgrade *immediately*.

(Bug #33814, CVE-2008-0226, CVE-2008-0227)

Changes in MySQL Enterprise 5.0.54 [MRU] (2007-12-14)

This is a *Monthly Rapid Update* release of the MySQL Enterprise Server 5.0.

This section documents all changes and bugfixes that have been applied since the last MySQL Enterprise Server release (5.0.52). If you would like to receive more fine-grained and personalized *update alerts* about fixes that are relevant to the version and features you use, please consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details please see <http://www.mysql.com/products/enterprise/advisors.html>.

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- The `mysql_odbc_escape_string()` C API function has been removed. It has multibyte character escaping issues, doesn't honor the `NO_BACKSLASH_ESCAPES` SQL mode and is not needed anymore by Connector/ODBC as of 3.51.17. (Bug #29592)

References: See also: Bug #41728.

- The argument for the `mysql-test-run.pl --do-test` and `--skip-test` options is now interpreted as a Perl regular expression if there is a pattern metacharacter in the argument value. This enables more flexible specification of which tests to perform or skip.

Bugs Fixed

- **Security Enhancement:** It was possible to force an error message of excessive length which could lead to a buffer overflow. This has been made no longer possible as a security precaution. (Bug #32707)
- **Performance:** InnoDB had a race condition for an adaptive hash rw-lock waiting for an X-lock. This fix may also provide significant speed improvements on systems experiencing problems with contention for the adaptive hash index. (Bug #29560)
- **Incompatible Change:** The MySQL 5.0.50 patch for this bug was reverted because it changed the behavior of a General Availability MySQL release. (Bug #30234)

References: See also: Bug #27525.

- **Incompatible Change:** It was possible for option files to be read twice at program startup, if some of the standard option file locations turned out to be the same directory. Now duplicates are removed from the list of files to be read.

Also, users could not override system-wide settings using `~/my.cnf` because `SYSCONFDIR/my.cnf` was read last. The latter file now is read earlier so that `~/my.cnf` can override system-wide settings.

The fix for this problem had a side effect such that on Unix, MySQL programs looked for options in `~/my.cnf` rather than the standard location of `~/my.cnf`. That problem is addressed in Bug #38180. (Bug #20748)

References: See also: Bug #38180.

- **Replication:** It was possible for the name of the relay log file to exceed the amount of memory reserved for it, possibly leading to a crash of the server. (Bug #31836)

References: See also: Bug #28597.

- **Replication:** Corruption of log events caused the server to crash on 64-bit Linux systems having 4 GB or more of memory. (Bug #31793)
- **Replication:** One thread could read uninitialized memory from the stack of another thread. This issue was only known to occur in a `mysqld` process acting as both a master and a slave. (Bug #30752)
- **Replication:** Due a previous change in how the default name and location of the binary log file were determined, replication failed following some upgrades. (Bug #28597, Bug #28603)

References: See also: Bug #31836. This issue is a regression of: Bug #20166.

- **Replication:** Stored procedures having `BIT` parameters were not replicated correctly. (Bug #26199)
- **Replication:** Issuing `SHOW SLAVE STATUS` as `mysqld` was shutting down could cause a crash. (Bug #26000)
- **Replication:** An `UPDATE` statement using a stored function that modified a nontransactional table was not logged if it failed. This caused the copy of the nontransactional table on the master have a row that the copy on the slave did not.

In addition, when an `INSERT ... ON DUPLICATE KEY UPDATE` statement encountered a duplicate key constraint, but the `UPDATE` did not actually change any data, the statement was not logged. As a result of this fix, such statements are now treated the same for logging purposes as other `UPDATE` statements, and so are written to the binary log. (Bug #23333)

References: See also: Bug #12713.

- **Replication:** A replication slave sometimes failed to reconnect because it was unable to run `SHOW SLAVE HOSTS`. It was not necessary to run this statement on slaves (since the master should track connection IDs), and the execution of this statement by slaves was removed. (Bug #21132)

References: See also: Bug #13963, Bug #21869.

- An `ORDER BY` query using `IS NULL` in the `WHERE` clause did not return correct results. (Bug #32815)
- The `LAST_DAY()` function returns a `DATE` value, but internally the value did not have the time fields zeroed and calculations involving the value could return incorrect results. (Bug #32770)
- Use of the `cp932` character set with `CAST()` in an `ORDER BY` clause could cause a server crash. (Bug #32726)
- A subquery using an `IS NULL` check of a column defined as `NOT NULL` in a table used in the `FROM` clause of the outer query produced an invalid result. (Bug #32694)
- Specifying a nonexistent column for an `INSERT DELAYED` statement caused a server crash rather than producing an error. (Bug #32676)
- Use of `CLIENT_MULTI_QUERIES` caused `libmysqld` to crash. (Bug #32624)
- The `INTERVAL()` function incorrectly handled `NULL` values in the value list. (Bug #32560)

- Use of a `NULL`-returning `GROUP BY` expression in conjunction with `WITH ROLLUP` could cause a server crash. (Bug #32558)
References: See also: Bug #31095.
- A `SELECT ... GROUP BY bit_column` query failed with an assertion if the length of the `BIT` column used for the `GROUP BY` was not an integer multiple of 8. (Bug #32556)
- Using `SELECT INTO OUTFILE` with 8-bit `ENCLOSED BY` characters led to corrupted data when the data was reloaded using `LOAD DATA INFILE`. This was because `SELECT INTO OUTFILE` failed to escape the 8-bit characters. (Bug #32533)
- For `FLUSH TABLES WITH READ LOCK`, the server failed to properly detect write-locked tables when running with low-priority updates, resulting in a crash or deadlock. (Bug #32528)
- Sending several `KILL QUERY` statements to target a connection running `SELECT SLEEP()` could freeze the server. (Bug #32436)
- `ssl-cipher` values in option files were not being read by `libmysqlclient`. (Bug #32429)
- Repeated execution of a query containing a `CASE` expression and numerous `AND` and `OR` relations could crash the server. The root cause of the issue was determined to be that the internal `SEL_ARG` structure was not properly initialized when created. (Bug #32403)
- Referencing within a subquery an alias used in the `SELECT` list of the outer query was incorrectly permitted. (Bug #32400)
- An `ORDER BY` query on a view created using a `FEDERATED` table as a base table caused the server to crash. (Bug #32374)
- Comparison of a `BIGINT NOT NULL` column with a constant arithmetic expression that evaluated to `NULL` mistakenly caused the error `Column '...' cannot be null` (error 1048). (Bug #32335)
- Assigning a 65,536-byte string to a `TEXT` column (which can hold a maximum of 65,535 bytes) resulted in truncation without a warning. Now a truncation warning is generated. (Bug #32282)
- `MIN()` and `MAX()` could return incorrect results when an index was present if a loose index scan was used. (Bug #32268)
- Memory corruption could occur due to large index map in `Range checked for each record` status reported by `EXPLAIN SELECT`. The problem was based in an incorrectly calculated length of the buffer used to store a hexadecimal representation of an index map, which could result in buffer overrun and stack corruption under some circumstances. (Bug #32241)
- Various test program cleanups were made: 1) `mytest` and `libmysqltest` were removed. 2) `bug25714` displays an error message when invoked with incorrect arguments or the `--help` option. 3) `mysql_client_test` exits cleanly with a proper error status. (Bug #32221)
- For comparisons of the form `date_col OP datetime_const` (where `OP` is `=`, `<`, `>`, `<=`, or `>=`), the comparison is done using `DATETIME` values, per the fix for Bug #27590. However that fix caused any index on `date_col` not to be used and compromised performance. Now the index is used again. (Bug #32198)
References: See also: Bug #27590.
- `DATETIME` arguments specified in numeric form were treated by `DATE_ADD()` as `DATE` values. (Bug #32180)

- `InnoDB` does not support `SPATIAL` indexes, but could crash when asked to handle one. Now an error is returned. (Bug #32125)
- With `lower_case_table_names` set, `CREATE TABLE LIKE` was treated differently by `libmysqld` than by the nonembedded server. (Bug #32063)
- Within a subquery, `UNION` was handled differently than at the top level, which could result in incorrect results or a server crash. (Bug #32036, Bug #32051)
- Changing the SQL mode to cause dates with “zero” parts to be considered invalid (such as `'1000-00-00'`) could result in indexed and nonindexed searches returning different results for a column that contained such dates. (Bug #31928)
- `ucs2` does not work as a client character set, but attempts to use it as such were not rejected. Now `character_set_client` cannot be set to `ucs2`. This also affects statements such as `SET NAMES` and `SET CHARACTER SET`. (Bug #31615)
- Killing a `CREATE TABLE ... LIKE` statement that was waiting for a name lock caused a server crash. When the statement was killed, the server attempted to release locks that were not held. (Bug #31479)
- `myisamchk --unpack` could corrupt a table that when unpacked has static (fixed-length) row format. (Bug #31277)
- Server variables could not be set to their current values on Linux platforms. (Bug #31177)
References: See also: Bug #6958.
- Data in `BLOB` or `GEOMETRY` columns could be cropped when performing a `UNION` query. (Bug #31158)
- The server crashed in the parser when running out of memory. Memory handling in the parser has been improved to gracefully return an error when out-of-memory conditions occur in the parser. (Bug #31153)
- MySQL declares a `UNIQUE` key as a `PRIMARY` key if it doesn't have `NULL` columns and is not a partial key, and the `PRIMARY` key must always be the first key. However, in some cases, a nonfirst key could be reported as `PRIMARY`, leading to an assert failure by `InnoDB`. This is fixed by correcting the key sort order. (Bug #31137)
- `REGEXP` operations could cause a server crash for character sets such as `ucs2`. Now the arguments are converted to `utf8` if possible, to permit correct results to be produced if the resulting strings contain only 8-bit characters. (Bug #31081)
- Many nested subqueries in a single query could lead to excessive memory consumption and possibly a crash of the server. (Bug #31048)
- The optimizer incorrectly optimized conditions out of the `WHERE` clause in some queries involving subqueries and indexed columns. (Bug #30788)
- Improper calculation of `CASE` expression results could lead to value truncation. (Bug #30782)
- A multiple-table `UPDATE` involving transactional and nontransactional tables caused an assertion failure. (Bug #30763)
- `mysql-test-run.pl` could not run `mysqld` with `root` privileges. (Bug #30630)
- The options available to the `CHECK TABLE` statement were also permitted in `OPTIMIZE TABLE` and `ANALYZE TABLE` statements, but caused corruption during their execution. These options were never supported for these statements, and an error is now raised if you try to apply these options to these statements. (Bug #30495)

- When casting a string value to an integer, cases where the input string contained a decimal point and was long enough to overrun the `unsigned long long` type were not handled correctly. The position of the decimal point was not taken into account which resulted in miscalculated numbers and incorrect truncation to appropriate SQL data type limits. (Bug #30453)
- For `CREATE ... SELECT ... FROM`, where the resulting table contained indexes, adding `SQL_BUFFER_RESULT` to the `SELECT` part caused index corruption in the table. (Bug #30384)
- The optimizer made incorrect assumptions about the value of the `is_member` value for user-defined functions, sometimes resulting in incorrect ordering of UDF results. (Bug #30355)
- Some valid `euc-kr` characters having the second byte in the ranges `[0x41..0x5A]` and `[0x61..0x7A]` were rejected. (Bug #30315)
- Simultaneous `ALTER TABLE` statements for `BLACKHOLE` tables caused 100% CPU use due to locking problems. (Bug #30294)
- Tables with a `GEOMETRY` column could be marked as corrupt if you added a non-`SPATIAL` index on a `GEOMETRY` column. (Bug #30284)
- On some 64-bit systems, inserting the largest negative value into a `BIGINT` column resulted in incorrect data. (Bug #30069)
- The `mysql` client program now ignores Unicode byte order mark (BOM) characters at the beginning of input files. Previously, it read them and sent them to the server, resulting in a syntax error.

Presence of a BOM does not cause `mysql` to change its default character set. To do that, invoke `mysql` with an option such as `--default-character-set=utf8`. (Bug #29323)

- For transactional tables, an error during a multiple-table `DELETE` statement did not roll back the statement. (Bug #29136)
- Denormalized double-precision numbers cannot be handled properly by old MIPS processors. For IRIX, this is now handled by enabling a mode to use a software workaround. (Bug #29085)
- When doing a `DELETE` on a table that involved a `JOIN` with `MyISAM` or `MERGE` tables and the `JOIN` referred to the same table, the operation could fail reporting `ERROR 1030 (HY000): Got error 134 from storage engine`. This was because scans on the table contents would change because of rows that had already been deleted. (Bug #28837)
- A race condition between killing a statement and the thread executing the statement could lead to a situation such that the binary log contained an event indicating that the statement was killed, whereas the statement actually executed to completion. (Bug #27571)
- Some queries using the `NAME_CONST()` function failed to return either a result or an error to the client, causing it to hang. This was due to the fact that there was no check to insure that both arguments to this function were constant expressions. (Bug #27545, Bug #32559)
- `mysqld` sometimes miscalculated the number of digits required when storing a floating-point number in a `CHAR` column. This caused the value to be truncated, or (when using a debug build) caused the server to crash. (Bug #26788)

References: See also: Bug #12860.

- If the expected precision of an arithmetic expression exceeded the maximum precision supported by MySQL, the precision of the result was reduced by an unpredictable or arbitrary amount, rather than to the maximum precision. In some cases, exceeding the maximum supported precision could also lead to a crash of the server. (Bug #24907)

- Zero-padding of exponent values was not the same across platforms. (Bug #12860)
- If an `INSERT ... SELECT` statement is executed, and no automatically generated value is successfully inserted, then `mysql_insert_id()` returns the ID of the last inserted row.

If no automatically generated value is successfully inserted, then `mysql_insert_id()` returns 0. (Bug #9481)

Changes in MySQL Enterprise 5.0.52 [MRU] (2007-11-30)

This is a *Monthly Rapid Update* release of the MySQL Enterprise Server 5.0.

This section documents all changes and bugfixes that have been applied since the last MySQL Enterprise Server release (5.0.50). If you would like to receive more fine-grained and personalized *update alerts* about fixes that are relevant to the version and features you use, please consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details please see <http://www.mysql.com/products/enterprise/advisors.html>.

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- `mysqldump` produces a `-- Dump completed on DATE` comment at the end of the dump if `-- comments` is given. The date causes dump files for identical data take at different times to appear to be different. The new options `--dump-date` and `--skip-dump-date` control whether the date is added to the comment. `--skip-dump-date` suppresses date printing. The default is `--dump-date` (include the date in the comment). (Bug #31077)
- The default value of the `connect_timeout` system variable was increased from 5 to 10 seconds. This might help in cases where clients frequently encounter errors of the form `Lost connection to MySQL server at 'XXX', system error: errno.` (Bug #28359)
- The use of InnoDB hash indexes now can be controlled by setting the new `innodb_adaptive_hash_index` system variable at server startup. By default, this variable is enabled. See [Adaptive Hash Indexes](#).

Bugs Fixed

- **Security Fix:** Using `RENAME TABLE` against a table with explicit `DATA DIRECTORY` and `INDEX DIRECTORY` options can be used to overwrite system table information by replacing the symbolic link points. the file to which the symlink points.

MySQL will now return an error when the file to which the symlink points already exists. (Bug #32111, CVE-2007-5969)
- **Security Fix:** `ALTER VIEW` retained the original `DEFINER` value, even when altered by another user, which could enable that user to gain the access rights of the view. Now `ALTER VIEW` is permitted only to the original definer or users with the `SUPER` privilege. (Bug #29908)
- **Security Fix:** When using a `FEDERATED` table, the local server could be forced to crash if the remote server returned a result with fewer columns than expected. (Bug #29801)
- **Incompatible Change:** With `ONLY_FULL_GROUP_BY` SQL mode enabled, queries such as `SELECT a FROM t1 HAVING COUNT(*) > 2` were not being rejected as they should have been.

This fix results in the following behavior:

- There is a check against mixing group and nongroup columns *only* when `ONLY_FULL_GROUP_BY` is enabled.
- This check is done both for the select list and for the `HAVING` clause if there is one.

This behavior differs from previous versions as follows:

- Previously, the `HAVING` clause was not checked when `ONLY_FULL_GROUP_BY` was enabled; now it is checked.
- Previously, the select list was checked even when `ONLY_FULL_GROUP_BY` was not enabled; now it is checked only when `ONLY_FULL_GROUP_BY` is enabled.

(Bug #31794)

- **Incompatible Change:** It was possible to create a view having a column whose name consisted of an empty string or space characters only.

One result of this bug fix is that aliases for columns in the view `SELECT` statement are checked to ensure that they are legal column names. In particular, the length must be within the maximum column length of 64 characters, not the maximum alias length of 256 characters. This can cause problems for replication or loading dump files. For additional information and workarounds, see [Restrictions on Views](#). (Bug #27695)

References: See also: Bug #31202.

- **Incompatible Change:** Several type-preserving functions and operators returned an incorrect result type that does not match their argument types: `COALESCE()`, `IF()`, `IFNULL()`, `LEAST()`, `GREATEST()`, `CASE`. These now aggregate using the precise SQL types of their arguments rather than the internal type. In addition, the result type of the `STR_TO_DATE()` function is now `DATETIME` by default. (Bug #27216)
- **MySQL Cluster:** An uninitialized variable in the `NDB` storage engine code led to `AUTO_INCREMENT` failures when the server was compiled with `gcc` 4.2.1. (Bug #31848)

References: This issue is a regression of: Bug #27437.

- **MySQL Cluster:** An error with an `if` statement in `sql/ha_ndbcluster.cc` could potentially lead to an infinite loop in case of failure when working with `AUTO_INCREMENT` columns in `NDB` tables. (Bug #31810)
- **MySQL Cluster:** The `NDB` storage engine code was not safe for strict-alias optimization in `gcc` 4.2.1. (Bug #31761)
- **MySQL Cluster:** Transaction timeouts were not handled well in some circumstances, leading to excessive number of transactions being aborted unnecessarily. (Bug #30379)
- **MySQL Cluster:** In some cases, the cluster management server logged entries multiple times following a restart of `ndb_mgmd`. (Bug #29565)
- **MySQL Cluster:** An interpreted program of sufficient size and complexity could cause all cluster data nodes to shut down due to buffer overruns. (Bug #29390)
- **MySQL Cluster:** `UPDATE IGNORE` could sometimes fail on `NDB` tables due to the use of uninitialized data when checking for duplicate keys to be ignored. (Bug #25817)

- **Replication:** Use of the `@hostname` system variable in inserts in `mysql_system_tables_data.sql` did not replicate. The workaround is to select its value into a user variable (which does replicate) and insert that. (Bug #31167)
- A build problem introduced in MySQL 5.0.52 was resolved: The x86 32-bit Intel `icc`-compiled server binary had unwanted dependences on Intel `icc` runtime libraries. (Bug #32514)
- The rules for valid column names were being applied differently for base tables and views. (Bug #32496)
- The default grant tables on Windows contained information for host `production.mysql.com`, which should not be there. (Bug #32219)
- Under certain conditions, the presence of a `GROUP BY` clause could cause an `ORDER BY` clause to be ignored. (Bug #32202)
- The server crashed on optimizations involving a join of `INT` and `MEDIUMINT` columns and a system variable in the `WHERE` clause. (Bug #32103)
- User-defined functions are not loaded if the server is started with the `--skip-grant-tables` option, but the server did not properly handle this case and issued an `Out of memory` error message instead. (Bug #32020)
- A column with malformed multibyte characters could cause the full-text parser to go into an infinite loop. (Bug #31950)
- In debug builds, testing the result of an `IN` subquery against `NULL` caused an assertion failure. (Bug #31884)
- Comparison results for `BETWEEN` were different from those for operators like `<` and `>` for `DATETIME`-like values with trailing extra characters such as `'2007-10-01 00:00:00 GMT-6'`. `BETWEEN` treated the values as `DATETIME`, whereas the other operators performed a binary-string comparison. Now they all uniformly use a `DATETIME` comparison, but generate warnings for values with trailing garbage. (Bug #31800)
- The server could crash during `filesort` for `ORDER BY` based on expressions with `INET_NTOA()` or `OCT()` if those functions returned `NULL`. (Bug #31758)
- For a fatal error during a `filesort` in `find_all_keys()`, the error was returned without the necessary handler uninitialization, causing an assertion failure. (Bug #31742)
- The examined-rows count was not incremented for `const` queries. (Bug #31700)
- The `mysql_change_user()` C API function was subject to buffer overflow. (Bug #31669)
- For `SELECT ... INTO OUTFILE`, if the `ENCLOSED BY` string is empty and the `FIELDS TERMINATED BY` string started with a special character (one of `n`, `t`, `r`, `b`, `0`, `Z`, or `N`), every occurrence of the character within field values would be duplicated. (Bug #31663)
- `SHOW COLUMNS` and `DESCRIBE` displayed `null` as the column type for a view with no valid definer. This caused `mysqldump` to produce a nonreloadable dump file for the view. (Bug #31662)
- The `mysqlbug` script did not include the correct values of `CFLAGS` and `CXXFLAGS` that were used to configure the distribution. (Bug #31644)
- A buffer used when setting variables was not dimensioned to accommodate the trailing `'\0'` byte, so a single-byte buffer overrun was possible. (Bug #31588)
- `HAVING` could treat lettercase of table aliases incorrectly if `lower_case_table_names` was enabled. (Bug #31562)

- The fix for Bug #24989 introduced a problem such that a `NULL` thread handler could be used during a rollback operation. This problem is unlikely to be seen in practice. (Bug #31517)
- The length of the result from `IFNULL()` could be calculated incorrectly because the sign of the result was not taken into account. (Bug #31471)
- Queries that used the `ref` access method or index-based subquery execution over indexes that have `DECIMAL` columns could fail with an error `Column col_name cannot be null`. (Bug #31450)
- `SELECT 1 REGEX NULL` caused an assertion failure for debug servers. (Bug #31440)
- Executing `RENAME` while tables were open for use with `HANDLER` statements could cause a server crash. (Bug #31409)
- `mysql-test-run.pl` tried to create files in a directory where it could not be expected to have write permission. `mysqltest` created `.reject` files in a directory other than the one where test results go. (Bug #31398)
- `DROP USER` caused an increase in memory usage. (Bug #31347)
- For an almost-full `MyISAM` table, an insert that failed could leave the table in a corrupt state. (Bug #31305)
- `CONVERT(val, DATETIME)` failed on invalid input, but processing was not aborted for the `WHERE` clause, leading to a server crash. (Bug #31253)
- Allocation of an insufficiently large group-by buffer following creation of a temporary table could lead to a server crash. (Bug #31249)
- Use of `DECIMAL(n, n) ZEROFILL` in `GROUP_CONCAT()` could cause a server crash. (Bug #31227)
- With small values of `myisam_sort_buffer_size`, `REPAIR TABLE` for `MyISAM` tables could cause a server crash. (Bug #31174)
- If `MAKETIME()` returned `NULL` when used in an `ORDER BY` that was evaluated using `filesort`, a server crash could result. (Bug #31160)
- Full-text searches on `ucs2` columns caused a server crash. (`FULLTEXT` indexes on `ucs2` columns cannot be used, but it should be possible to perform `IN BOOLEAN MODE` searches on `ucs2` columns without a crash.) (Bug #31159)
- An assertion designed to detect a bug in the `ROLLUP` implementation would incorrectly be triggered when used in a subquery context with noncacheable statements. (Bug #31156)
- Selecting spatial types in a `UNION` could cause a server crash. (Bug #31155)
- Use of `GROUP_CONCAT(DISTINCT bit_column)` caused an assertion failure. (Bug #31154)
- `GROUP BY NULL WITH ROLLUP` could cause a server crash. (Bug #31095)

References: See also: Bug #32558.

- Internal conversion routines could fail for several multibyte character sets (`big5`, `cp932`, `euckr`, `gb2312`, `sjis`) for empty strings or during evaluation of `SOUNDS LIKE`. (Bug #31069, Bug #31070)
- The `MOD()` function and the `%` operator crashed the server for a divisor less than 1 with a very long fractional part. (Bug #31019)
- On Windows, the `pthread_mutex_trylock()` implementation was incorrect. (Bug #30992)

- A character set introducer followed by a hexadecimal or bit-value literal did not check its argument and could return an ill-formed result for invalid input. (Bug #30986)
- `CHAR(str USING charset)` did not check its argument and could return an ill-formed result for invalid input. (Bug #30982)
- The result from `CHAR(str USING ucs2)` did not add a leading 0x00 byte for input strings with an odd number of bytes. (Bug #30981)
- The `GeomFromText()` function could cause a server crash if the first argument was `NULL` or the empty string. (Bug #30955)
- `MAKEDATE()` incorrectly moved year values in the 100 to 200 range into the 1970 to 2069 range. (This is legitimate for 00 to 99, but three-digit years should be used unchanged.) (Bug #30951)
- When invoked with constant arguments, `STR_TO_DATE()` could use a cached value for the format string and return incorrect results. (Bug #30942)
- `GROUP_CONCAT()` returned `' , '` rather than an empty string when the argument column contained only empty strings. (Bug #30897)
- For `MEMORY` tables, lookups for `NULL` values in `BTREE` indexes could return incorrect results. (Bug #30885)
- Calling `NAME_CONST()` with nonconstant arguments triggered an assertion failure. Nonconstant arguments are no longer permitted. (Bug #30832)
- For a spatial column with a regular (non-`SPATIAL`) index, queries failed if the optimizer tried to use the index. (Bug #30825)
- Values for the `--tc-heuristic-recover` option incorrectly were treated as values for the `--myisam-stats-method` option. (Bug #30821)
- On Windows, the `pthread_mutex_trylock()` implementation was incorrect. One symptom was that invalidating the query cache could cause a server crash. (Bug #30768)
- Under some circumstances, `CREATE TABLE ... SELECT` could crash the server or incorrectly report that the table row size was too large. (Bug #30736)
- Using the `MIN()` or `MAX()` function to select one part of a multi-part key could cause a crash when the function result was `NULL`. (Bug #30715)
- The optimizer could ignore `ORDER BY` in cases when the result set is ordered by `filesort`, resulting in rows being returned in incorrect order. (Bug #30666)
- `MyISAM` tables could not exceed $4294967295 (2^{32} - 1)$ rows on Windows. (Bug #30638)
- For `MEMORY` tables, `DELETE` statements that remove rows based on an index read could fail to remove all matching rows. (Bug #30590)
- Using `GROUP BY` on an expression of the form `timestamp_col DIV number` caused a server crash due to incorrect calculation of number of decimals. (Bug #30587)
- When expanding a `*` in a `USING` or `NATURAL` join, the check for table access for both tables in the join was done using only the grant information of the first table. (Bug #30468)
- Versions of `mysqldump` from MySQL 4.1 or higher tried to use `START TRANSACTION WITH CONSISTENT SNAPSHOT` if the `--single-transaction` and `--master-data` options were given, even with servers older than 4.1 that do not support consistent snapshots. (Bug #30444)

- Setting certain values on a table using a spatial index could cause the server to crash. (Bug #30286)
- Some `INFORMATION_SCHEMA` tables are intended for internal use, but could be accessed by using `SHOW` statements. (Bug #30079)
- Under some circumstances, a UDF initialization function could be passed incorrect argument lengths. (Bug #29804)
- Specifying the `--without-geometry` option for `configure` caused server compilation to fail. (Bug #29772)
- `configure` did not find `nss` on some Linux platforms. (Bug #29658)
- The `log` and `log_slow_queries` system variables were displayed by `SHOW VARIABLES` but could not be accessed in expressions as `@@log` and `@@log_slow_queries`. Also, attempting to set them with `SET` produced an incorrect `Unknown system variable` message. Now these variables can be accessed in expressions and attempting to set their values produces an error message that the variable is read only. (Bug #29131)
- `SHOW VARIABLES` did not display the `relay_log`, `relay_log_index`, or `relay_log_info_file` system variables. (Bug #28893)
- On Windows, `mysql_upgrade` created temporary files in `C:\` and did not clean them up. (Bug #28774)
- Index hints specified in view definitions were ignored when using the view to select from the base table. (Bug #28702)
- Views do not have indexes, so index hints do not apply. Use of index hints when selecting from a view is no longer permitted. (Bug #28701)
- After changing the SQL mode to a restrictive value that would make already inserted dates in a column be considered invalid, searches returned different results depending on whether the column was indexed. (Bug #28687)
- The result from `CHAR()` was incorrectly assumed in some contexts to return a single-byte result. (Bug #28550)
- The parser confused user-defined function (UDF) and stored function creation for `CREATE FUNCTION` and required that there be a default database when creating UDFs, although there is no such requirement. (Bug #28318, Bug #29816)
- The result of a comparison between `VARBINARY` and `BINARY` columns differed depending on whether the `VARBINARY` column was indexed. (Bug #28076)
- The metadata in some `MYSQL_FIELD` members could be incorrect when a temporary table was used to evaluate a query. (Bug #27990)
- `comp_err` created files with permissions such that they might be inaccessible during `make install` operations. (Bug #27789)
- The anonymous accounts were not being created during MySQL installation. (Bug #27692)
- Using `FLUSH TABLES` in one connection while another connection is using `HANDLER` statements caused a server crash.

**Note**

This fix supersedes a fix made previously in MySQL 5.0.32 and reverted in MySQL 5.0.48.

(Bug #21587)

References: See also: Bug #29474.

- Host names sometimes were treated as case sensitive in account-management statements (`CREATE USER`, `GRANT`, `REVOKE`, and so forth). (Bug #19828)
- The `readline` library has been updated to version 5.2. This addresses issues in the `mysql` client where history and editing within the client failed to work as expected. (Bug #18431)
- The `Aborted_clients` status variable was incremented twice if a client exited without calling `mysql_close()`. (Bug #16918)
- Clients were ignoring the TCP/IP port number specified as the default port using the `--with-tcp-port` configuration option. (Bug #15327)
- Values of types `REAL ZEROFILL`, `DOUBLE ZEROFILL`, `FLOAT ZEROFILL`, were not zero-filled when converted to a character representation in the C prepared statement API. (Bug #11589)
- `mysql` stripped comments from statements sent to the server. Now the `--comments` or `--skip-comments` option can be used to control whether to retain or strip comments. The default is `--skip-comments`. (Bug #11230, Bug #26215)
- Several buffer-size system variables were either being handled incorrectly for large values (for settings larger than 4GB, they were truncated to values less than 4GB without a warning), or were limited unnecessarily to 4GB even on 64-bit systems. The following changes were made:
 - For `key_buffer_size`, values larger than 4GB are permitted on 64-bit platforms (except Windows, for which large values are truncated to 4GB with a warning).
 - For `join_buffer_size`, `sort_buffer_size`, and `myisam_sort_buffer_size`, values are limited to 4GB on all platforms. Larger values are truncated to 4GB with a warning.

In addition, settings for `read_buffer_size` and `read_rnd_buffer_size` are limited to 2GB on all platforms. Larger values are truncated to 2GB with a warning. (Bug #5731, Bug #29419, Bug #29446)

- Executing `DISABLE KEYS` and `ENABLE KEYS` on a nonempty table would cause the size of the index file for the table to grow considerable. This was because the `DISABLE KEYS` operation would only mark the existing index, without deleting the index blocks. The `ENABLE KEYS` operation would re-create the index, adding new blocks, while the previous index blocks would remain. Existing indexes are now dropped and recreated when the `ENABLE KEYS` statement is executed. (Bug #4692)

Changes in MySQL Community Server 5.0.51b (2008-04-24)

This is a bugfix release for the current MySQL Community Server production release family. It replaces MySQL 5.0.51.

Bugs Fixed

- On Windows, the installer attempted to use JScript to determine whether the target data directory already existed. On Windows Vista x64, this resulted in an error because the installer was attempting to run the JScript in a 32-bit engine, which wasn't registered on Vista. The installer no longer uses JScript but instead relies on a native WiX command. (Bug #36103)
- The MySQL preferences pane did not work to start or stop MySQL on Mac OS X 10.5 (Leopard). (Bug #28854)

- On Mac OS X, the StartupItem for MySQL did not work. (Bug #25008)

Changes in MySQL Community Server 5.0.51a (2008-01-11)

This is a bugfix release for the current MySQL Community Server production release family. It replaces MySQL 5.0.51.

Bugs Fixed

- **Security Fix:** Three vulnerabilities in yaSSL versions 1.7.5 and earlier were discovered that could lead to a server crash or execution of unauthorized code. The exploit requires a server with yaSSL enabled and TCP/IP connections enabled, but does not require valid MySQL account credentials. The exploit does not apply to OpenSSL.



Warning

The proof-of-concept exploit is freely available on the Internet. Everyone with a vulnerable MySQL configuration is advised to upgrade *immediately*.

(Bug #33814, CVE-2008-0226, CVE-2008-0227)

- **Security Fix:** `ALTER VIEW` retained the original `DEFINER` value, even when altered by another user, which could enable that user to gain the access rights of the view. Now `ALTER VIEW` is permitted only to the original definer or users with the `SUPER` privilege. (Bug #29908)
- **Security Fix:** When using a `FEDERATED` table, the local server could be forced to crash if the remote server returned a result with fewer columns than expected. (Bug #29801)
- When running the MySQL Instance Configuration Wizard, a race condition could exist that failed to connect to a newly configured instance. This was because `mysqld` had not completed the startup process before the next stage of the installation process. (Bug #28628)
- For Vista installs, `MySQLInstanceConfig.exe` did not add the default MySQL port to the firewall exceptions. It now provides a check box that enables the user a choice of whether to do this. (Bug #24853)
- For Windows Vista, `MySQLInstanceConfig.exe` did not include a proper manifest enabling it to run with administrative privileges. (Bug #22563)

References: See also: Bug #24732.

- `MySQLInstanceConfig.exe` failed to grant certain privileges to the `'root'@'%'` account. (Bug #17303)

Changes in MySQL Community Server 5.0.51 (2007-11-15)

This is a bugfix release for the current MySQL Community Server production release family. It replaces MySQL 5.0.45.

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- **Incompatible Change:** The parser accepted statements that contained `/* ... */` that were not properly closed with `*/`, such as `SELECT 1 /* + 2`. Statements that contain unclosed `/*`-comments now are rejected with a syntax error.

This fix has the potential to cause incompatibilities. Because of Bug #26302, which caused the trailing `*/` to be truncated from comments in views, stored routines, triggers, and events, it is possible that objects of those types may have been stored with definitions that now will be rejected as syntactically invalid. Such objects should be dropped and re-created so that their definitions do not contain truncated comments. If a stored object definition contains only a single statement (does not use a `BEGIN ... END` block) and contains a comment within the statement, the comment should be moved to follow the statement or the object should be rewritten to use a `BEGIN ... END` block. For example, this statement:

```
CREATE PROCEDURE p() SELECT 1 /* my comment */ ;
```

Can be rewritten in either of these ways:

```
CREATE PROCEDURE p() SELECT 1; /* my comment */
CREATE PROCEDURE p() BEGIN SELECT 1 /* my comment */ ; END;
```

(Bug #28779)

- **MySQL Cluster:** Mapping of `NDB` error codes to MySQL storage engine error codes has been improved. (Bug #28423)
- **MySQL Cluster:** `auto_increment_increment` and `auto_increment_offset` are now supported for `NDB` tables. (Bug #26342)
- **MySQL Cluster:** The output from the cluster management client showing the progress of data node starts has been improved. (Bug #23354)
- **Replication:** The `sql_mode`, `foreign_key_checks`, `unique_checks`, character set/collations, and `sql_auto_is_null` session variables are written to the binary log and honored during replication. See [The Binary Log](#).
- Server parser performance was improved for expression parsing by lowering the number of state transitions and reductions needed. (Bug #30625)
- Server parser performance was improved for boolean expressions. (Bug #30237)
- If a `MyISAM` table is created with no `DATA DIRECTORY` option, the `.MYD` file is created in the database directory. By default, if `MyISAM` finds an existing `.MYD` file in this case, it overwrites it. The same applies to `.MYI` files for tables created with no `INDEX DIRECTORY` option. To suppress this behavior, start the server with the new `--keep_files_on_create` option, in which case `MyISAM` will not overwrite existing files and returns an error instead. (Bug #29325)
- `SHOW COLUMNS` now returns `NULL` instead of the empty string for the `Default` value of columns that have no `DEFAULT` clause specified. (Bug #27747)
- MySQL source distributions are now available in Zip format. (Bug #27742)
- If a `MERGE` table cannot be opened or used because of a problem with an underlying table, `CHECK TABLE` now displays information about which table caused the problem. (Bug #26976)
- The `EXAMPLE` storage engine is now enabled by default.

Bugs Fixed

- **Security Fix:** Using `RENAME TABLE` against a table with explicit `DATA DIRECTORY` and `INDEX DIRECTORY` options can be used to overwrite system table information by replacing the symbolic link points. the file to which the symlink points.

MySQL will now return an error when the file to which the symlink points already exists. (Bug #32111, CVE-2007-5969)

- **Incompatible Change:** The file `mysqld.exe` was mistakenly included in binary distributions between MySQL 5.0.42 and 5.0.48. You should use `mysqld-nt.exe`. (Bug #32197)
- **Incompatible Change:** Multiple-table `DELETE` statements containing ambiguous aliases could have unintended side effects such as deleting rows from the wrong table. Example:

```
DELETE FROM t1 AS a2 USING t1 AS a1 INNER JOIN t2 AS a2;
```

This bug fix enables aliases to be declared only in the `table_references` part. Elsewhere in the statement, alias references are permitted but not alias declarations. However, this patch was reverted in MySQL 5.0.54 because it changed the behavior of a General Availability MySQL release. (Bug #30234)

References: See also: Bug #27525.

- **Incompatible Change:** Failure to consider collation when comparing space characters could result in incorrect index entry order, leading to incorrect comparisons, inability to find some index values, misordered index entries, misordered `ORDER BY` results, or tables that `CHECK TABLE` reports as having corrupt indexes.

As a result of this bug fix, indexes must be rebuilt for columns that use any of these character sets: `eucjpm`, `euc_kr`, `gb2312`, `latin7`, `macce`, `ujis`. See [Checking Whether Tables or Indexes Must Be Rebuilt](#). (Bug #29461)

- **MySQL Cluster; Packaging:** Some commercial MySQL Cluster RPM packages included support for the `InnoDB` storage engine. (`InnoDB` is not part of the standard commercial MySQL Cluster offering.) (Bug #31989)
- **MySQL Cluster:** Attempting to restore a backup made on a cluster host using one endian to a machine using the other endian could cause the cluster to fail. (Bug #29674)
- **MySQL Cluster:** When restarting a data node, queries could hang during that node's start phase 5, and continue only after the node had entered phase 6. (Bug #29364)
- **MySQL Cluster:** Replica redo logs were inconsistently handled during a system restart. (Bug #29354)
- **MySQL Cluster:** Reads on `BLOB` columns were not locked when they needed to be to guarantee consistency. (Bug #29102)

References: See also: Bug #31482.

- **MySQL Cluster:** A query using joins between several large tables and requiring unique index lookups failed to complete, eventually returning `Unknown Error` after a very long period of time. This occurred due to inadequate handling of instances where the Transaction Coordinator ran out of `TransactionBufferMemory`, when the cluster should have returned NDB error code 4012 (`Request ndbd time-out`). (Bug #28804)
- **MySQL Cluster:** The description of the `--print` option provided in the output from `ndb_restore --help` was incorrect. (Bug #27683)
- **MySQL Cluster:** The management client's response to `START BACKUP WAIT COMPLETED` did not include the backup ID. (Bug #27640)
- **MySQL Cluster:** An invalid subselect on an `NDB` table could cause `mysqld` to crash. (Bug #27494)

- **MySQL Cluster:** An attempt to perform a `SELECT ... FROM INFORMATION_SCHEMA.TABLES` whose result included information about `NDB` tables for which the user had no privileges crashed the MySQL Server on which the query was performed. (Bug #26793)
- **MySQL Cluster:** Warnings and errors generated by `ndb_config --config-file=file` were sent to `stdout`, rather than to `stderr`. (Bug #25941)
- **MySQL Cluster:** Large file support did not work in AIX server binaries. (Bug #10776)
- **Replication:** The thread ID was not reset properly after execution of `mysql_change_user()`, which could cause replication failure when replicating temporary tables. (Bug #29734)
- **Replication:** Operations that used the time zone replicated the time zone only for successful operations, but did not replicate the time zone for errors that need to know it. (Bug #29536)
- **Replication:** `INSERT DELAYED` statements on a master server are replicated as non-`DELAYED` inserts on slaves (which is normal, to preserve serialization), but the inserts on the slave did not use concurrent inserts. Now `INSERT DELAYED` on a slave is converted to a concurrent insert when possible, and to a normal insert otherwise. (Bug #29152)
- **Replication:** `DROP USER` statements that named multiple users, only some of which could be dropped, were replicated incorrectly. (Bug #29030)
- **Replication:** An error that happened inside `INSERT`, `UPDATE`, or `DELETE` statements performed from within a stored function or trigger could cause inconsistency between master and slave servers. (Bug #27417)
- **Replication:** Slave servers could incorrectly interpret an out-of-memory error from the master and reconnect using the wrong binary log position. (Bug #24192)
- When a `TIMESTAMP` with a nonzero time part was converted to a `DATE` value, no warning was generated. This caused index lookups to assume that this is a valid conversion and was returning rows that match a comparison between a `TIMESTAMP` value and a `DATE` keypart. Now a warning is generated so that `TIMESTAMP` with a nonzero time part will not match `DATE` values. (Bug #31221)
- A server crash could occur when a non-`DETERMINISTIC` stored function was used in a `GROUP BY` clause. (Bug #31035)
- For an `InnoDB` table if a `SELECT` was ordered by the primary key and also had a `WHERE field = value` clause on a different field that was indexed, a `DESC` order instruction would be ignored. (Bug #31001)
- A failed `HANDLER ... READ` operation could leave the table in a locked state. (Bug #30632)
- The optimization that uses a unique index to remove `GROUP BY` did not ensure that the index was actually used, thus violating the `ORDER BY` that is implied by `GROUP BY`. (Bug #30596)
- `SHOW STATUS LIKE 'Ssl_cipher_list'` from a MySQL client connected using SSL returned an empty string rather than a list of available ciphers. (Bug #30593)
- Memory corruption occurred for some queries with a top-level `OR` operation in the `WHERE` condition if they contained equality predicates and other sargable predicates in disjunctive parts of the condition. (Bug #30396)
- Issuing a `DELETE` statement having both an `ORDER BY` clause and a `LIMIT` clause could cause `mysqld` to crash. (Bug #30385)

- The `Last_query_cost` status variable value can be computed accurately only for simple “flat” queries, not complex queries such as those with subqueries or `UNION`. However, the value was not consistently being set to 0 for complex queries. (Bug #30377)
- Queries that had a `GROUP BY` clause and selected `COUNT(DISTINCT bit_column)` returned incorrect results. (Bug #30324)
- The server created temporary tables for filesort operations in the working directory, not in the directory specified by the `tmpdir` system variable. (Bug #30287)
- The query cache does not support retrieval of statements for which column level access control applies, but the server was still caching such statements, thus wasting memory. (Bug #30269)
- Using `DISTINCT` or `GROUP BY` on a `BIT` column in a `SELECT` statement caused the column to be cast internally as an integer, with incorrect results being returned from the query. (Bug #30245)
- `GROUP BY` on `BIT` columns produced incorrect results. (Bug #30219)
- Using `KILL QUERY` or `KILL CONNECTION` to kill a `SELECT` statement caused a server crash if the query cache was enabled. (Bug #30201)
- Prepared statements containing `CONNECTION_ID()` could be written improperly to the binary log. (Bug #30200)
- When a thread executing a `DROP TABLE` statement was killed, the table name locks that had been acquired were not released. (Bug #30193)
- Short-format `mysql` commands embedded within `/*! ... */` comments were parsed incorrectly by `mysql`, which discarded the rest of the comment including the terminating `*/` characters. The result was a malformed (unclosed) comment. Now `mysql` does not discard the `*/` characters. (Bug #30164)
- When `mysqldump` wrote `DROP DATABASE` statements within version-specific comments, it included the terminating semicolon in the wrong place, causing following statements to fail when the dump file was reloaded. (Bug #30126)
- Use of local variables with non-ASCII names in stored procedures crashed the server. (Bug #30120)
- On Windows, client libraries lacked symbols required for linking. (Bug #30118)
- `--myisam-recover=` (empty option value) did not disable `MyISAM` recovery. (Bug #30088)
- The `IS_UPDATABLE` column in the `INFORMATION_SCHEMA.VIEWS` table was not always set correctly. (Bug #30020)
- Statements within stored procedures ignored the value of the `low_priority_updates` system variable. (Bug #29963)

References: See also: Bug #26162.

- For `MyISAM` tables on Windows, `INSERT`, `DELETE`, or `UPDATE` followed by `ALTER TABLE` within `LOCK TABLES` could cause table corruption. (Bug #29957)
- With auto-reconnect enabled, row fetching for a prepared statement could crash after reconnect occurred because loss of the statement handler was not accounted for. (Bug #29948)
- `LOCK TABLES` did not pre-lock tables used in triggers of the locked tables. Unexpected locking behavior and statement failures similar to `failed: 1100: Table 'xx' was not locked with LOCK TABLES` could result. (Bug #29929)

- `INSERT ... VALUES(CONNECTION_ID(), ...)` statements were written to the binary log in such a way that they could not be properly restored. (Bug #29928)
- Adding `DISTINCT` could cause incorrect rows to appear in a query result. (Bug #29911)
- Using the `DATE()` function in a `WHERE` clause did not return any records after encountering `NULL`. However, using `TRIM()` or `CAST()` produced the correct results. (Bug #29898)
- Very long prepared statements in stored procedures could cause a server crash. (Bug #29856)
- If query execution involved a temporary table, `GROUP_CONCAT()` could return a result with an incorrect character set. (Bug #29850)
- If one thread was performing concurrent inserts, other threads reading from the same table using equality key searches could see the index values for new rows before the data values had been written, leading to reports of table corruption. (Bug #29838)
- Repeatedly accessing a view in a stored procedure (for example, in a loop) caused a small amount of memory to be allocated per access. Although this memory is deallocated on disconnect, it could be a problem for a long running stored procedures that make repeated access of views. (Bug #29834)
- `mysqldump` produced output that incorrectly discarded the `NO_AUTO_VALUE_ON_ZERO` value of the `sql_mode` variable after dumping triggers. (Bug #29788)
- For `MEMORY` tables, the `index_merge` union access method could return incorrect results. (Bug #29740)
- Comparison of `TIME` values using the `BETWEEN` operator led to string comparison, producing incorrect results in some cases. Now the values are compared as integers. (Bug #29739)
- For a table with a `DATE` column `date_col` such that selecting rows with `WHERE date_col = 'date_val 00:00:00'` yielded a nonempty result, adding `GROUP BY date_col` caused the result to be empty. (Bug #29729)
- In some cases, `INSERT INTO ... SELECT ... GROUP BY` could insert rows even if the `SELECT` by itself produced an empty result. (Bug #29717)
- For the embedded server, the `mysql_stmt_store_result()` C API function caused a memory leak for empty result sets. (Bug #29687)
- `EXPLAIN` produced `Impossible where` for statements of the form `SELECT ... FROM t WHERE c=0`, where `c` was an `ENUM` column defined as a primary key. (Bug #29661)
- On Windows, `ALTER TABLE` hung if records were locked in share mode by a long-running transaction. (Bug #29644)
- A left join between two views could produce incorrect results. (Bug #29604)
- Certain statements with unions, subqueries, and joins could result in huge memory consumption. (Bug #29582)
- Clients using SSL could hang the server. (Bug #29579)
- A slave running with `--log-slave-updates` failed to write `INSERT DELAY IGNORE` statements to its binary log, resulting in different binary log contents on the master and slave. (Bug #29571)
- An incorrect result was returned when comparing string values that were converted to `TIME` values with `CAST()`. (Bug #29555)
- `gcov` coverage-testing information was not written if the server crashed. (Bug #29543)

- In the `ascii` character set, conversion of DEL (0x7F) to Unicode incorrectly resulted in QUESTION MARK (0x3F) rather than DEL. (Bug #29499)
- A field packet with `NULL` fields caused a `libmysqlclient` crash. (Bug #29494)
- When using a combination of `HANDLER... READ` and `DELETE` on a table, MySQL continued to open new copies of the table every time, leading to an exhaustion of file descriptors. (Bug #29474)
References: This issue is a regression of: Bug #21587.
- On Windows, the `mysql` client died if the user entered a statement and Return after entering **Control+C**. (Bug #29469)
- Corrupt data resulted from use of `SELECT ... INTO OUTFILE 'file_name' FIELDS ENCLOSED BY 'c'`, where `c` is a digit or minus sign, followed by `LOAD DATA INFILE 'file_name' FIELDS ENCLOSED BY 'c'`. (Bug #29442)
- Killing an `INSERT DELAYED` thread caused a server crash. (Bug #29431)
- Use of `SHOW BINLOG EVENTS` for a nonexistent log file followed by `PURGE BINARY LOGS` caused a server crash. (Bug #29420)
- Assertion failure could occur for grouping queries that employed `DECIMAL` user variables with assignments to them. (Bug #29417)
- For `CAST(expr AS DECIMAL(M,D))`, the limits of 65 and 30 on the precision (`M`) and scale (`D`) were not enforced. (Bug #29415)
- If a view used a function in its `SELECT` statement, the columns from the view were not inserted into the `INFORMATION_SCHEMA.COLUMNS` table. (Bug #29408)
- Results for a select query that aliases the column names against a view could duplicate one column while omitting another. This bug could occur for a query over a multiple-table view that includes an `ORDER BY` clause in its definition. (Bug #29392)
- `mysqldump` created a stray file when a given a too-long file name argument. (Bug #29361)
- The special “zero” `ENUM` value was coerced to the normal empty string `ENUM` value during a column-to-column copy. This affected `CREATE ... SELECT` statements and `SELECT` statements with aggregate functions on `ENUM` columns in the `GROUP BY` clause. (Bug #29360)
- Optimization of queries with `DETERMINISTIC` stored functions in the `WHERE` clause was ineffective: A sequential scan was always used. (Bug #29338)
- `MyISAM` corruption could occur with the `cp932_japanese_ci` collation for the `cp932` character set due to incorrect comparison for trailing space. (Bug #29333)
- The `mysql_list_fields()` C API function incorrectly set `MYSQL_FIELD::decimals` for some view columns. (Bug #29306)
- `FULLTEXT` indexes could be corrupted by certain `gbk` characters. (Bug #29299)
- `SELECT ... INTO OUTFILE` followed by `LOAD DATA` could result in garbled characters when the `FIELDS ENCLOSED BY` clause named a delimiter of `'0'`, `'b'`, `'n'`, `'r'`, `'t'`, `'N'`, or `'Z'` due to an interaction of character encoding and doubling for data values containing the enclosed-by character. (Bug #29294)
- Sort order of the collation wasn't used when comparing trailing spaces. This could lead to incorrect comparison results, incorrectly created indexes, or incorrect result set order for queries that include an `ORDER BY` clause. (Bug #29261)

- If an `ENUM` column contained `' '` as one of its members (represented with numeric value greater than 0), and the column contained error values (represented as 0 and displayed as `' '`), using `ALTER TABLE` to modify the column definition caused the 0 values to be given the numeric value of the nonzero `' '` member. (Bug #29251)
- Calling `mysql_options()` after `mysql_real_connect()` could cause clients to crash. (Bug #29247)
- `CHECK TABLE` for `ARCHIVE` tables could falsely report table corruption or cause a server crash. (Bug #29207)
- Mixing binary and `utf8` columns in a union caused field lengths to be calculated incorrectly, resulting in truncation. (Bug #29205)
- `AsText()` could fail with a buffer overrun. (Bug #29166)
- `InnoDB` refused to start on some versions of FreeBSD with LinuxThreads. This is fixed by enabling file locking on FreeBSD. (Bug #29155)
- `LOCK TABLES` was not atomic when more than one `InnoDB` tables were locked. (Bug #29154)
- A network structure was initialized incorrectly, leading to embedded server crashes. (Bug #29117)
- An assertion failure occurred if a query contained a conjunctive predicate of the form `view_column = constant` in the `WHERE` clause and the `GROUP BY` clause contained a reference to a different view column. The fix also enables application of an optimization that was being skipped if a query contained a conjunctive predicate of the form `view_column = constant` in the `WHERE` clause and the `GROUP BY` clause contained a reference to the same view column. (Bug #29104)
- A maximum of 4TB `InnoDB` free space was reported by `SHOW TABLE STATUS`, which is incorrect on systems with more than 4TB space. (Bug #29097)
- If an `INSERT INTO ... SELECT` statement inserted into the same table that the `SELECT` retrieved from, and the `SELECT` included `ORDER BY` and `LIMIT` clauses, different data was inserted than the data produced by the `SELECT` executed by itself. (Bug #29095)
- Queries that performed a lookup into a `BINARY` index containing key values ending with spaces caused an assertion failure for debug builds and incorrect results for nondebug builds. (Bug #29087)
- The semantics of `BIGINT` depended on platform-specific characteristics. (Bug #29079)
- A byte-order issue in writing a spatial index to disk caused bad index files on some systems. (Bug #29070)
- If one of the queries in a `UNION` used the `SQL_CACHE` option and another query in the `UNION` contained a nondeterministic function, the result was still cached. For example, this query was incorrectly cached:

```
SELECT NOW() FROM t1 UNION SELECT SQL_CACHE 1 FROM t1;
```

(Bug #29053)

- Creation of a legal stored procedure could fail if no default database had been selected. (Bug #29050)
- `REPLACE`, `INSERT IGNORE`, and `UPDATE IGNORE` did not work for `FEDERATED` tables. (Bug #29019)
- Inserting into `InnoDB` tables and executing `RESET MASTER` in multiple threads cause assertion failure in debug server binaries. (Bug #28983)
- For a `ucs2` column, `GROUP_CONCAT()` did not convert separators to the result character set before inserting them, producing a result containing a mixture of two different character sets. (Bug #28925)

- Queries using UDFs or stored functions were cached. (Bug #28921)
- For a join with `GROUP BY` or `ORDER BY` and a view reference in the `FROM` list, the query metadata erroneously showed empty table aliases and database names for the view columns. (Bug #28898)
- Coercion of ASCII values to character sets that are a superset of ASCII sometimes was not done, resulting in `illegal mix of collations` errors. These cases now are resolved using repertoire, a new string expression attribute (see [String Repertoire](#)). (Bug #28875)
- Non-utf8 characters could get mangled when stored in `CSV` tables. (Bug #28862)
- `ALTER VIEW` is not supported as a prepared statement but was not being rejected. `ALTER VIEW` is now prohibited as a prepared statement or when called within stored routines. (Bug #28846)
- In strict SQL mode, errors silently stopped the SQL thread even for errors named using the `--slave-skip-errors` option. (Bug #28839)
- Fast `ALTER TABLE` (that works without rebuilding the table) acquired duplicate locks in the storage engine. In `MyISAM`, if `ALTER TABLE` was issued under `LOCK TABLE`, it caused all data inserted after `LOCK TABLE` to disappear. (Bug #28838)
- Killing an SSL connection on platforms where MySQL is compiled with `-DSIGNAL_WITH_VIO_CLOSE` (Windows, Mac OS X, and some others) could crash the server. (Bug #28812)
- Runtime changes to the `log_queries_not_using_indexes` system variable were ignored. (Bug #28808)
- Tables using the `InnoDB` storage engine incremented `AUTO_INCREMENT` values incorrectly with `ON DUPLICATE KEY UPDATE`. (Bug #28781)
- Selecting a column not present in the selected-from table caused an extra error to be produced by `SHOW ERRORS`. (Bug #28677)
- For a statement of the form `CREATE t1 SELECT integer_constant`, the server created the column using the `DECIMAL` data type for large negative values that are within the range of `BIGINT`. (Bug #28625)
- For `InnoDB` tables, MySQL unnecessarily sorted records in certain cases when the records were retrieved by `InnoDB` in the proper order already. (Bug #28591)
- A `SELECT` in one connection could be blocked by `INSERT ... ON DUPLICATE KEY UPDATE` in another connection even when `low_priority_updates` is set. (Bug #28587)
- `mysql_install_db` could fail to find script files that it needs. (Bug #28585)
- When one thread attempts to lock two (or more) tables and another thread executes a statement that aborts these locks (such as `REPAIR TABLE`, `OPTIMIZE TABLE`, or `CHECK TABLE`), the thread might get a table object with an incorrect lock type in the table cache. The result is table corruption or a server crash. (Bug #28574)
- `mysql_upgrade` could run binaries dynamically linked against incorrect versions of shared libraries. (Bug #28560)
- If a stored procedure was created and invoked prior to selecting a default database with `USE`, a `No database selected` error occurred. (Bug #28551)
- On Mac OS X, shared-library installation path names were incorrect. (Bug #28544)
- Using the `--skip-add-drop-table` option with `mysqldump` generated incorrect SQL if the database included any views. The recreation of views requires the creation and removal of temporary tables. This

option suppressed the removal of those temporary tables. The same applied to `--compact` since this option also invokes `--skip-add-drop-table`. (Bug #28524)

- `mysqlbinlog --hexdump` generated incorrect output due to omission of the “#” comment character for some comment lines. (Bug #28293)
- A race condition in the interaction between `MyISAM` and the query cache code caused the query cache not to invalidate itself for concurrently inserted data. (Bug #28249)
- Indexing column prefixes in `InnoDB` tables could cause table corruption. (Bug #28138)
- Index creation could fail due to truncation of key values to the maximum key length rather than to a multiple of the maximum character length. (Bug #28125)
- The `LOCATE()` function returned `NULL` if any of its arguments evaluated to `NULL`. Likewise, the predicate, `LOCATE(str,NULL) IS NULL`, erroneously evaluated to `FALSE`. (Bug #27932)
- On Windows, symbols for `yaSSL` and `taocrypt` were missing from `mysqlclient.lib`, resulting in unresolved symbol errors for clients linked against that library. (Bug #27861)
- The modification of a table by a partially completed multi-column update was not recorded in the binlog, rather than being marked by an event and a corresponding error code. (Bug #27716)
- With recent versions of `DBD::mysql`, `mysqlhotcopy` generated table names that were doubly qualified with the database name. (Bug #27694)
- The anonymous accounts were not being created during MySQL installation. (Bug #27692)
- Some `SHOW` statements and `INFORMATION_SCHEMA` queries could expose information not permitted by the user's access privileges. (Bug #27629)
- A stack overrun could occur when storing `DATETIME` values using repeated prepared statements. (Bug #27592)
- Dropping a user-defined function could cause a server crash if the function was still in use by another thread. (Bug #27564)
- Some character mappings in the `ascii.xml` file were incorrect.

As a result of this bug fix, indexes must be rebuilt for columns that use the `ascii_general_ci` collation for columns that contain any of these characters: ``', '[', '\', ']', '~'`. See [Checking Whether Tables or Indexes Must Be Rebuilt](#). (Bug #27562)

- The parser rules for the `SHOW PROFILE` statement were revised to work with older versions of `bison`. (Bug #27433)
- Unsafe aliasing in the source caused a client library crash when compiled with `gcc 4` at high optimization levels. (Bug #27383)
- A `SELECT` with more than 31 nested dependent subqueries returned an incorrect result. (Bug #27352)
- Index-based range reads could fail for comparisons that involved contraction characters (such as `ch` in Czech or `ll` in Spanish). (Bug #27345)
- Aggregations in subqueries that refer to outer query columns were not always correctly referenced to the proper outer query. (Bug #27333)
- `INSERT INTO ... SELECT` caused a crash if `innodb_locks_unsafe_for_binlog` was enabled. (Bug #27294)

- Error returns from the `time()` system call were ignored. (Bug #27198)
- Phantom reads could occur under `InnoDB SERIALIZABLE` isolation level. (Bug #27197)
- The `SUBSTRING()` function returned the entire string instead of an empty string when it was called from a stored procedure and when the length parameter was specified by a variable with the value "0". (Bug #27130)
- `ALTER TABLE ... ENABLE KEYS` could cause `mysqld` to crash when executed on a table containing on a `MyISAM` table containing billions of rows. (Bug #27029)
- `FEDERATED` tables had an artificially low maximum of key length. (Bug #26909)
- Binary content `0x00` in a `BLOB` column sometimes became `0x5C 0x00` following a dump and reload, which could cause problems with data using multibyte character sets such as `GBK` (Chinese). This was due to a problem with `SELECT INTO OUTFILE` whereby `LOAD DATA` later incorrectly interpreted `0x5C` as the second byte of a multibyte sequence rather than as the `SOLIDUS` ("\`\`") character, used by MySQL as the escape character. (Bug #26711)
- Index creation could corrupt the table definition in the `.frm` file: 1) A table with the maximum number of key segments and maximum length key name would have a corrupted `.frm` file, due to incorrect calculation of the total key length. 2) `MyISAM` would reject a table with the maximum number of keys and the maximum number of key segments in all keys. (It would permit one less than this total maximum.) Now `MyISAM` accepts a table defined with the maximum. (Bug #26642)
- After the first read of a `TEMPORARY` table, `CHECK TABLE` could report the table as being corrupt. (Bug #26325)
- If an operation had an `InnoDB` table, and two triggers, `AFTER UPDATE` and `AFTER INSERT`, competing for different resources (such as two distinct `MyISAM` tables), the triggers were unable to execute concurrently. In addition, `INSERT` and `UPDATE` statements for the `InnoDB` table were unable to run concurrently. (Bug #26141)
- `ALTER DATABASE` did not require at least one option. (Bug #25859)
- Using `HANDLER` to open a table having a storage engine not supported by `HANDLER` properly returned an error, but also improperly prevented the table from being dropped by other connections. (Bug #25856)
- The index merge union access algorithm could produce incorrect results with `InnoDB` tables. The problem could also occur for queries that used `DISTINCT`. (Bug #25798)
- When using a `FEDERATED` table, the value of `LAST_INSERT_ID()` would not correctly update the C API interface, which would affect the autogenerated ID returned both through the C API and the MySQL protocol, affecting Connectors that used the protocol or C API. (Bug #25714)
- The server was blocked from opening other tables while the `FEDERATED` engine was attempting to open a remote table. Now the server does not check the correctness of a `FEDERATED` table at `CREATE TABLE` time, but waits until the table actually is accessed. (Bug #25679)
- Under ActiveState Perl, `mysql-test-run.pl` could kill itself when attempting to kill other processes. (Bug #25657)
- Several `InnoDB` assertion failures were corrected. (Bug #25645)
- A query with `DISTINCT` in the select list to which the loose-scan optimization for grouping queries was applied returned an incorrect result set when the query was used with the `SQL_BIG_RESULT` option. (Bug #25602)

- For a multiple-row insert into a `FEDERATED` table that refers to a remote transactional table, if the insert failed for a row due to constraint failure, the remote table would contain a partial commit (the rows preceding the failed one) instead of rolling back the statement completely. This occurred because the rows were treated as individual inserts.

Now `FEDERATED` performs bulk-insert handling such that multiple rows are sent to the remote table in a batch. This provides a performance improvement and enables the remote table to perform statement rollback properly should an error occur. This capability has the following limitations:

- The size of the insert cannot exceed the maximum packet size between servers. If the insert exceeds this size, it is broken into multiple packets and the rollback problem can occur.
- Bulk-insert handling does not occur for `INSERT ... ON DUPLICATE KEY UPDATE`.

(Bug #25513)

- The `FEDERATED` storage engine failed silently for `INSERT ... ON DUPLICATE KEY UPDATE` if a duplicate key violation occurred. `FEDERATED` does not support `ON DUPLICATE KEY UPDATE`, so now it correctly returns an `ER_DUP_KEY` error if a duplicate key violation occurs. (Bug #25511)
- For `InnoDB` tables, `CREATE TABLE a AS SELECT * FROM A` failed. (Bug #25164)
- In a stored function or trigger, when `InnoDB` detected deadlock, it attempted rollback and displayed an incorrect error message (`Explicit or implicit commit is not permitted in stored function or trigger`). Now `InnoDB` returns an error under these conditions and does not attempt rollback. Rollback is handled outside of `InnoDB` above the function/trigger level. (Bug #24989)
- A too-long `shared-memory-base-name` value could cause a buffer overflow and crash the server or clients. (Bug #24924)
- Dropping a temporary `InnoDB` table that had been locked with `LOCK TABLES` caused a server crash. (Bug #24918)
- On Windows, executables did not include Vista manifests. (Bug #24732)

References: See also: Bug #22563.

- If MySQL/`InnoDB` crashed very quickly after starting up, it would not force a checkpoint. In this case, `InnoDB` would skip crash recovery at next startup, and the database would become corrupt. Now, if the redo log scan at `InnoDB` startup goes past the last checkpoint, crash recovery is forced. (Bug #23710)
- The server deducted some bytes from the `key_cache_block_size` option value and reduced it to the next lower 512 byte boundary. The resulting block size was not a power of two. Setting the `key_cache_block_size` system variable to a value that is not a power of two resulted in `MyISAM` table corruption. (Bug #23068, Bug #28478, Bug #25853)
- `SHOW INNODB STATUS` caused an assertion failure under high load. (Bug #22819)
- `SHOW BINLOG EVENTS` displayed incorrect values of `End_log_pos` for events associated with transactional storage engines. (Bug #22540)
- A statement of the form `CREATE TABLE IF NOT EXISTS t1 SELECT f1() AS i` failed with a deadlock error if the stored function `f1()` referred to a table with the same name as the to-be-created table. Now it correctly produces a message that the table already exists. (Bug #22427)
- Read lock requests that were blocked by a pending write lock request were not permitted to proceed if the statement requesting the write lock was killed. (Bug #21281)

- Under heavy load with a large query cache, invalidating part of the cache could cause the server to freeze (that is, to be unable to service other operations until the invalidation was complete). (Bug #21074)

References: See also: Bug #39253.

- `mysql-stress-test.pl` and `mysqld_multi.server.sh` were missing from some binary distributions. (Bug #21023, Bug #25486)
- On Windows, the server used 10MB of memory for each connection thread, resulting in memory exhaustion. Now each thread uses 1MB. (Bug #20815)
- Worked around an `icc` problem with an incorrect machine instruction being generated in the context of software pre-fetching after a subroutine got in-lined. (Upgrading to `icc` 10.0.026 makes the workaround unnecessary.) (Bug #20803)
- InnoDB produced an unnecessary (and harmless) warning: `InnoDB: Error: trying to declare trx to enter InnoDB, but InnoDB: it already is declared.` (Bug #20090)
- Under ActiveState Perl, `mysql-test-run.pl` would not run. (Bug #18415)
- The server crashed when the size of an `ARCHIVE` table grew larger than 2GB. (Bug #15787)
- `SQL_BIG_RESULT` had no effect for `CREATE TABLE ... SELECT SQL_BIG_RESULT ...` statements. (Bug #15130)
- On 64-bit Windows systems, the Config Wizard failed to complete the setup because 64-bit Windows does not resolve dynamic linking of the 64-bit `libmysql.dll` to a 32-bit application like the Config Wizard. (Bug #14649)
- `mysql_setpermission` tried to grant global-only privileges at the database level. (Bug #14618)
- Parameters of type `DATETIME` or `DATE` in stored procedures were silently converted to `VARBINARY`. (Bug #13675)
- For the general query log, logging of prepared statements executed using the C API differed from logging of prepared statements performed with `PREPARE` and `EXECUTE`. Logging for the latter was missing the `Prepare` and `Execute` lines. (Bug #13326)
- The server returned data from `SHOW CREATE TABLE` statement or a `SELECT` statement on an `INFORMATION_SCHEMA` table using the `binary` character set. (Bug #10491)
- Backup software can cause `ERROR_SHARING_VIOLATION` or `ERROR_LOCK_VIOLATION` conditions during file operations. InnoDB now retries forever until the condition goes away. (Bug #9709)

Changes in MySQL Enterprise 5.0.50sp1a [QSP] (2008-01-11)

This is a *Service Pack* release of the MySQL Enterprise Server 5.0.

This is a bugfix release that replaces MySQL 5.0.50sp1.

Bugs Fixed

- **Security Fix:** Three vulnerabilities in yaSSL versions 1.7.5 and earlier were discovered that could lead to a server crash or execution of unauthorized code. The exploit requires a server with yaSSL enabled and TCP/IP connections enabled, but does not require valid MySQL account credentials. The exploit does not apply to OpenSSL.

**Warning**

The proof-of-concept exploit is freely available on the Internet. Everyone with a vulnerable MySQL configuration is advised to upgrade *immediately*.

(Bug #33814, CVE-2008-0226, CVE-2008-0227)

Changes in MySQL Enterprise 5.0.50sp1 [QSP] (2007-12-12)

This is a *Service Pack* release of the MySQL Enterprise Server 5.0.

This section documents all changes and bugfixes that have been applied since the last MySQL Enterprise Server release (5.0.50). If you would like to receive more fine-grained and personalized *update alerts* about fixes that are relevant to the version and features you use, please consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details please see <http://www.mysql.com/products/enterprise/advisors.html>.

Bugs Fixed

- **Security Fix:** Using `RENAME TABLE` against a table with explicit `DATA DIRECTORY` and `INDEX DIRECTORY` options can be used to overwrite system table information by replacing the symbolic link points. the file to which the symlink points.

MySQL will now return an error when the file to which the symlink points already exists. (Bug #32111, CVE-2007-5969)
- **Security Fix:** `ALTER VIEW` retained the original `DEFINER` value, even when altered by another user, which could enable that user to gain the access rights of the view. Now `ALTER VIEW` is permitted only to the original definer or users with the `SUPER` privilege. (Bug #29908)
- **Security Fix:** When using a `FEDERATED` table, the local server could be forced to crash if the remote server returned a result with fewer columns than expected. (Bug #29801)
- **Performance:** `InnoDB` had a race condition for an adaptive hash rw-lock waiting for an X-lock. This fix may also provide significant speed improvements on systems experiencing problems with contention for the adaptive hash index. (Bug #29560)
- A build problem introduced in MySQL 5.0.52 was resolved: The x86 32-bit Intel `icc`-compiled server binary had unwanted dependences on Intel `icc` runtime libraries. (Bug #32514)
- `InnoDB` does not support `SPATIAL` indexes, but could crash when asked to handle one. Now an error is returned. (Bug #32125)
- `mysql-test-run.pl` could not run `mysqld` with `root` privileges. (Bug #30630)

Changes in MySQL Enterprise 5.0.50 [MRU] (2007-10-19)

This is a *Monthly Rapid Update* release of the MySQL Enterprise Server 5.0.

This section documents all changes and bugfixes that have been applied since the last MySQL Enterprise Server release (5.0.48). If you would like to receive more fine-grained and personalized *update alerts* about fixes that are relevant to the version and features you use, please consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details please see <http://www.mysql.com/products/enterprise/advisors.html>.

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- **Incompatible Change:** The parser accepted statements that contained `/* ... */` that were not properly closed with `*/`, such as `SELECT 1 /* + 2`. Statements that contain unclosed `/*`-comments now are rejected with a syntax error.

This fix has the potential to cause incompatibilities. Because of Bug #26302, which caused the trailing `*/` to be truncated from comments in views, stored routines, triggers, and events, it is possible that objects of those types may have been stored with definitions that now will be rejected as syntactically invalid. Such objects should be dropped and re-created so that their definitions do not contain truncated comments. If a stored object definition contains only a single statement (does not use a `BEGIN ... END` block) and contains a comment within the statement, the comment should be moved to follow the statement or the object should be rewritten to use a `BEGIN ... END` block. For example, this statement:

```
CREATE PROCEDURE p() SELECT 1 /* my comment */ ;
```

Can be rewritten in either of these ways:

```
CREATE PROCEDURE p() SELECT 1; /* my comment */
CREATE PROCEDURE p() BEGIN SELECT 1 /* my comment */ ; END;
```

(Bug #28779)

- **MySQL Cluster:** Mapping of `NDB` error codes to MySQL storage engine error codes has been improved. (Bug #28423)
- **MySQL Cluster:** The output from the cluster management client showing the progress of data node starts has been improved. (Bug #23354)
- Server parser performance was improved for expression parsing by lowering the number of state transitions and reductions needed. (Bug #30625)
- Server parser performance was improved for boolean expressions. (Bug #30237)
- `SHOW COLUMNS` now returns `NULL` instead of the empty string for the `Default` value of columns that have no `DEFAULT` clause specified. (Bug #27747)

Bugs Fixed

- **Incompatible Change:** The file `mysqld.exe` was mistakenly included in binary distributions between MySQL 5.0.42 and 5.0.48. You should use `mysqld-nt.exe`. (Bug #32197)
- **Incompatible Change:** Multiple-table `DELETE` statements containing ambiguous aliases could have unintended side effects such as deleting rows from the wrong table. Example:

```
DELETE FROM t1 AS a2 USING t1 AS a1 INNER JOIN t2 AS a2;
```

This fix enables aliases to be declared only in the `table_references` part. Elsewhere in the statement, alias references are permitted but not alias declarations. However, this patch was reverted in MySQL 5.0.54 because it changed the behavior of a General Availability MySQL release. (Bug #30234)

References: See also: Bug #27525.

- **MySQL Cluster; Packaging:** Some commercial MySQL Cluster RPM packages included support for the [InnoDB](#) storage engine. ([InnoDB](#) is not part of the standard commercial MySQL Cluster offering.) (Bug #31989)
- **MySQL Cluster:** Attempting to restore a backup made on a cluster host using one endian to a machine using the other endian could cause the cluster to fail. (Bug #29674)
- **MySQL Cluster:** Reads on [BLOB](#) columns were not locked when they needed to be to guarantee consistency. (Bug #29102)

References: See also: Bug #31482.

- **MySQL Cluster:** A query using joins between several large tables and requiring unique index lookups failed to complete, eventually returning [Unknown Error](#) after a very long period of time. This occurred due to inadequate handling of instances where the Transaction Coordinator ran out of [TransactionBufferMemory](#), when the cluster should have returned NDB error code 4012 ([Request ndbd time-out](#)). (Bug #28804)
- **MySQL Cluster:** The description of the `--print` option provided in the output from `ndb_restore --help` was incorrect. (Bug #27683)
- **MySQL Cluster:** An invalid subselect on an [NDB](#) table could cause `mysqld` to crash. (Bug #27494)
- **MySQL Cluster:** An attempt to perform a `SELECT ... FROM INFORMATION_SCHEMA.TABLES` whose result included information about [NDB](#) tables for which the user had no privileges crashed the MySQL Server on which the query was performed. (Bug #26793)
- When a [TIMESTAMP](#) with a nonzero time part was converted to a [DATE](#) value, no warning was generated. This caused index lookups to assume that this is a valid conversion and was returning rows that match a comparison between a [TIMESTAMP](#) value and a [DATE](#) keypart. Now a warning is generated so that [TIMESTAMP](#) with a nonzero time part will not match [DATE](#) values. (Bug #31221)
- A server crash could occur when a non-[DETERMINISTIC](#) stored function was used in a `GROUP BY` clause. (Bug #31035)
- For an [InnoDB](#) table if a `SELECT` was ordered by the primary key and also had a `WHERE field = value` clause on a different field that was indexed, a `DESC` order instruction would be ignored. (Bug #31001)
- A failed `HANDLER ... READ` operation could leave the table in a locked state. (Bug #30632)
- The optimization that uses a unique index to remove `GROUP BY` did not ensure that the index was actually used, thus violating the `ORDER BY` that is implied by `GROUP BY`. (Bug #30596)
- `SHOW STATUS LIKE 'Ssl_cipher_list'` from a MySQL client connected using SSL returned an empty string rather than a list of available ciphers. (Bug #30593)
- Issuing a `DELETE` statement having both an `ORDER BY` clause and a `LIMIT` clause could cause `mysqld` to crash. (Bug #30385)
- The `Last_query_cost` status variable value can be computed accurately only for simple “flat” queries, not complex queries such as those with subqueries or `UNION`. However, the value was not consistently being set to 0 for complex queries. (Bug #30377)
- Queries that had a `GROUP BY` clause and selected `COUNT(DISTINCT bit_column)` returned incorrect results. (Bug #30324)
- Using `DISTINCT` or `GROUP BY` on a `BIT` column in a `SELECT` statement caused the column to be cast internally as an integer, with incorrect results being returned from the query. (Bug #30245)

- Short-format `mysql` commands embedded within `/*! ... */` comments were parsed incorrectly by `mysql`, which discarded the rest of the comment including the terminating `*/` characters. The result was a malformed (unclosed) comment. Now `mysql` does not discard the `*/` characters. (Bug #30164)
 - When `mysqldump` wrote `DROP DATABASE` statements within version-specific comments, it included the terminating semicolon in the wrong place, causing following statements to fail when the dump file was reloaded. (Bug #30126)
 - If a view used a function in its `SELECT` statement, the columns from the view were not inserted into the `INFORMATION_SCHEMA.COLUMNS` table. (Bug #29408)
 - Killing an SSL connection on platforms where MySQL is compiled with `-DSIGNAL_WITH_VIO_CLOSE` (Windows, Mac OS X, and some others) could crash the server. (Bug #28812)
 - A `SELECT` in one connection could be blocked by `INSERT ... ON DUPLICATE KEY UPDATE` in another connection even when `low_priority_updates` is set. (Bug #28587)
 - `mysql_upgrade` could run binaries dynamically linked against incorrect versions of shared libraries. (Bug #28560)
 - With recent versions of `DBD::mysql`, `mysqlhotcopy` generated table names that were doubly qualified with the database name. (Bug #27694)
 - For `InnoDB` tables, `CREATE TABLE a AS SELECT * FROM A` failed. (Bug #25164)
 - Under heavy load with a large query cache, invalidating part of the cache could cause the server to freeze (that is, to be unable to service other operations until the invalidation was complete). (Bug #21074)
- References: See also: Bug #39253.
- Worked around an `icc` problem with an incorrect machine instruction being generated in the context of software pre-fetching after a subroutine got in-lined. (Upgrading to `icc` 10.0.026 makes the workaround unnecessary.) (Bug #20803)
 - Parameters of type `DATETIME` or `DATE` in stored procedures were silently converted to `VARBINARY`. (Bug #13675)

Changes in MySQL Enterprise 5.0.48 [MRU] (2007-08-27)

This is a *Monthly Rapid Update* release of the MySQL Enterprise Server 5.0.

This section documents all changes and bugfixes that have been applied since the last last MySQL Enterprise Server release (5.0.46). If you would like to receive more fine-grained and personalized *update alerts* about fixes that are relevant to the version and features you use, please consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details please see <http://www.mysql.com/products/enterprise/advisors.html>.



Important

This release was withdrawn from production and is no longer available.

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- If a `MyISAM` table is created with no `DATA DIRECTORY` option, the `.MYD` file is created in the database directory. By default, if `MyISAM` finds an existing `.MYD` file in this case, it overwrites it. The same applies to `.MYI` files for tables created with no `INDEX DIRECTORY` option. To suppress this behavior, start the server with the new `--keep_files_on_create` option, in which case `MyISAM` will not overwrite existing files and returns an error instead. (Bug #29325)
- MySQL source distributions are now available in Zip format. (Bug #27742)
- The `EXAMPLE` storage engine is now enabled by default.

Bugs Fixed

- **Incompatible Change:** Failure to consider collation when comparing space characters could result in incorrect index entry order, leading to incorrect comparisons, inability to find some index values, misordered index entries, misordered `ORDER BY` results, or tables that `CHECK TABLE` reports as having corrupt indexes.

As a result of this bug fix, indexes must be rebuilt for columns that use any of these character sets: `eucjpm`, `euc_kr`, `gb2312`, `latin7`, `macce`, `ujis`. See [Checking Whether Tables or Indexes Must Be Rebuilt](#). (Bug #29461)

- **MySQL Cluster:** Warnings and errors generated by `ndb_config --config-file=file` were sent to `stdout`, rather than to `stderr`. (Bug #25941)
- **MySQL Cluster:** When a cluster backup was terminated using the `ABORT BACKUP` command in the management client, a misleading error message `Backup aborted by application: Permanent error: Internal error` was returned. The error message returned in such cases now reads `Backup aborted by user request`. (Bug #21052)
- **MySQL Cluster:** Large file support did not work in AIX server binaries. (Bug #10776)
- **Replication:** `SHOW SLAVE STATUS` failed when slave I/O was about to terminate. (Bug #34305)
- **Replication:** The thread ID was not reset properly after execution of `mysql_change_user()`, which could cause replication failure when replicating temporary tables. (Bug #29734)
- **Replication:** Operations that used the time zone replicated the time zone only for successful operations, but did not replicate the time zone for errors that need to know it. (Bug #29536)
- **Replication:** `INSERT DELAYED` statements on a master server are replicated as non-`DELAYED` inserts on slaves (which is normal, to preserve serialization), but the inserts on the slave did not use concurrent inserts. Now `INSERT DELAYED` on a slave is converted to a concurrent insert when possible, and to a normal insert otherwise. (Bug #29152)
- **Replication:** An error that happened inside `INSERT`, `UPDATE`, or `DELETE` statements performed from within a stored function or trigger could cause inconsistency between master and slave servers. (Bug #27417)
- **Replication:** Slave servers could incorrectly interpret an out-of-memory error from the master and reconnect using the wrong binary log position. (Bug #24192)
- Memory corruption occurred for some queries with a top-level `OR` operation in the `WHERE` condition if they contained equality predicates and other sargable predicates in disjunctive parts of the condition. (Bug #30396)
- The server created temporary tables for filesort operations in the working directory, not in the directory specified by the `tmpdir` system variable. (Bug #30287)

- The query cache does not support retrieval of statements for which column level access control applies, but the server was still caching such statements, thus wasting memory. (Bug #30269)
- `GROUP BY` on `BIT` columns produced incorrect results. (Bug #30219)
- Using `KILL QUERY` or `KILL CONNECTION` to kill a `SELECT` statement caused a server crash if the query cache was enabled. (Bug #30201)
- Prepared statements containing `CONNECTION_ID()` could be written improperly to the binary log. (Bug #30200)
- When a thread executing a `DROP TABLE` statement was killed, the table name locks that had been acquired were not released. (Bug #30193)
- Use of local variables with non-ASCII names in stored procedures crashed the server. (Bug #30120)
- On Windows, client libraries lacked symbols required for linking. (Bug #30118)
- `--myisam-recover=`' ' (empty option value) did not disable `MyISAM` recovery. (Bug #30088)
- The `IS_UPDATABLE` column in the `INFORMATION_SCHEMA.VIEWS` table was not always set correctly. (Bug #30020)
- Statements within stored procedures ignored the value of the `low_priority_updates` system variable. (Bug #29963)

References: See also: Bug #26162.

- For `MyISAM` tables on Windows, `INSERT`, `DELETE`, or `UPDATE` followed by `ALTER TABLE` within `LOCK TABLES` could cause table corruption. (Bug #29957)
- With auto-reconnect enabled, row fetching for a prepared statement could crash after reconnect occurred because loss of the statement handler was not accounted for. (Bug #29948)
- `LOCK TABLES` did not pre-lock tables used in triggers of the locked tables. Unexpected locking behavior and statement failures similar to `failed: 1100: Table 'xx' was not locked with LOCK TABLES` could result. (Bug #29929)
- `INSERT ... VALUES(CONNECTION_ID(), ...)` statements were written to the binary log in such a way that they could not be properly restored. (Bug #29928)
- Adding `DISTINCT` could cause incorrect rows to appear in a query result. (Bug #29911)
- Using the `DATE()` function in a `WHERE` clause did not return any records after encountering `NULL`. However, using `TRIM()` or `CAST()` produced the correct results. (Bug #29898)
- Very long prepared statements in stored procedures could cause a server crash. (Bug #29856)
- If query execution involved a temporary table, `GROUP_CONCAT()` could return a result with an incorrect character set. (Bug #29850)
- If one thread was performing concurrent inserts, other threads reading from the same table using equality key searches could see the index values for new rows before the data values had been written, leading to reports of table corruption. (Bug #29838)
- Repeatedly accessing a view in a stored procedure (for example, in a loop) caused a small amount of memory to be allocated per access. Although this memory is deallocated on disconnect, it could be a problem for a long running stored procedures that make repeated access of views. (Bug #29834)

- `mysqldump` produced output that incorrectly discarded the `NO_AUTO_VALUE_ON_ZERO` value of the `sql_mode` variable after dumping triggers. (Bug #29788)
- An assertion failure occurred within yaSSL for very long keys. (Bug #29784)
References: See also: Bug #53463.
- For `MEMORY` tables, the `index_merge` union access method could return incorrect results. (Bug #29740)
- Comparison of `TIME` values using the `BETWEEN` operator led to string comparison, producing incorrect results in some cases. Now the values are compared as integers. (Bug #29739)
- For a table with a `DATE` column `date_col` such that selecting rows with `WHERE date_col = 'date_val 00:00:00'` yielded a nonempty result, adding `GROUP BY date_col` caused the result to be empty. (Bug #29729)
- In some cases, `INSERT INTO ... SELECT ... GROUP BY` could insert rows even if the `SELECT` by itself produced an empty result. (Bug #29717)
- For the embedded server, the `mysql_stmt_store_result()` C API function caused a memory leak for empty result sets. (Bug #29687)
- `EXPLAIN` produced `Impossible where` for statements of the form `SELECT ... FROM t WHERE c=0`, where `c` was an `ENUM` column defined as a primary key. (Bug #29661)
- On Windows, `ALTER TABLE` hung if records were locked in share mode by a long-running transaction. (Bug #29644)
- A left join between two views could produce incorrect results. (Bug #29604)
- Certain statements with unions, subqueries, and joins could result in huge memory consumption. (Bug #29582)
- Clients using SSL could hang the server. (Bug #29579)
- A slave running with `--log-slave-updates` failed to write `INSERT DELAY IGNORE` statements to its binary log, resulting in different binary log contents on the master and slave. (Bug #29571)
- An incorrect result was returned when comparing string values that were converted to `TIME` values with `CAST()`. (Bug #29555)
- In the `ascii` character set, conversion of `DEL (0x7F)` to Unicode incorrectly resulted in `QUESTION MARK (0x3F)` rather than `DEL`. (Bug #29499)
- A field packet with `NULL` fields caused a `libmysqlclient` crash. (Bug #29494)
- When using a combination of `HANDLER ... READ` and `DELETE` on a table, MySQL continued to open new copies of the table every time, leading to an exhaustion of file descriptors. (Bug #29474)
References: This issue is a regression of: Bug #21587.
- On Windows, the `mysql` client died if the user entered a statement and Return after entering **Control+C**. (Bug #29469)
- Killing an `INSERT DELAYED` thread caused a server crash. (Bug #29431)
- The special “zero” `ENUM` value was coerced to the normal empty string `ENUM` value during a column-to-column copy. This affected `CREATE ... SELECT` statements and `SELECT` statements with aggregate functions on `ENUM` columns in the `GROUP BY` clause. (Bug #29360)

- Optimization of queries with `DETERMINISTIC` stored functions in the `WHERE` clause was ineffective: A sequential scan was always used. (Bug #29338)
- `MyISAM` corruption could occur with the `cp932_japanese_ci` collation for the `cp932` character set due to incorrect comparison for trailing space. (Bug #29333)
- The `mysql_list_fields()` C API function incorrectly set `MYSQL_FIELD::decimals` for some view columns. (Bug #29306)
- `InnoDB` refused to start on some versions of FreeBSD with LinuxThreads. This is fixed by enabling file locking on FreeBSD. (Bug #29155)
- A maximum of 4TB `InnoDB` free space was reported by `SHOW TABLE STATUS`, which is incorrect on systems with more than 4TB space. (Bug #29097)
- A byte-order issue in writing a spatial index to disk caused bad index files on some systems. (Bug #29070)
- Creation of a legal stored procedure could fail if no default database had been selected. (Bug #29050)
- Coercion of ASCII values to character sets that are a superset of ASCII sometimes was not done, resulting in `illegal mix of collations` errors. These cases now are resolved using repertoire, a new string expression attribute (see [String Repertoire](#)). (Bug #28875)
- Fast `ALTER TABLE` (that works without rebuilding the table) acquired duplicate locks in the storage engine. In `MyISAM`, if `ALTER TABLE` was issued under `LOCK TABLE`, it caused all data inserted after `LOCK TABLE` to disappear. (Bug #28838)
- Tables using the `InnoDB` storage engine incremented `AUTO_INCREMENT` values incorrectly with `ON DUPLICATE KEY UPDATE`. (Bug #28781)
- Starting the server with an `innodb_force_recovery` value of 4 did not work. (Bug #28604)
- For `InnoDB` tables, MySQL unnecessarily sorted records in certain cases when the records were retrieved by `InnoDB` in the proper order already. (Bug #28591)
- `mysql_install_db` could fail to find script files that it needs. (Bug #28585)
- If a stored procedure was created and invoked prior to selecting a default database with `USE`, a `No database selected` error occurred. (Bug #28551)
- On Mac OS X, shared-library installation path names were incorrect. (Bug #28544)
- Using the `--skip-add-drop-table` option with `mysqldump` generated incorrect SQL if the database included any views. The recreation of views requires the creation and removal of temporary tables. This option suppressed the removal of those temporary tables. The same applied to `--compact` since this option also invokes `--skip-add-drop-table`. (Bug #28524)
- A race condition in the interaction between `MyISAM` and the query cache code caused the query cache not to invalidate itself for concurrently inserted data. (Bug #28249)
- Indexing column prefixes in `InnoDB` tables could cause table corruption. (Bug #28138)
- Index creation could fail due to truncation of key values to the maximum key length rather than to a multiple of the maximum character length. (Bug #28125)
- On Windows, symbols for `yaSSL` and `taocrypt` were missing from `mysqlclient.lib`, resulting in unresolved symbol errors for clients linked against that library. (Bug #27861)

- Some `SHOW` statements and `INFORMATION_SCHEMA` queries could expose information not permitted by the user's access privileges. (Bug #27629)
- Some character mappings in the `ascii.xml` file were incorrect.
As a result of this bug fix, indexes must be rebuilt for columns that use the `ascii_general_ci` collation for columns that contain any of these characters: ```, `'`, `['`, `\'`, `]`, `~`. See [Checking Whether Tables or Indexes Must Be Rebuilt](#). (Bug #27562)
- A `SELECT` with more than 31 nested dependent subqueries returned an incorrect result. (Bug #27352)
- `INSERT INTO ... SELECT` caused a crash if `innodb_locks_unsafe_for_binlog` was enabled. (Bug #27294)
- `FEDERATED` tables had an artificially low maximum of key length. (Bug #26909)
- After the first read of a `TEMPORARY` table, `CHECK TABLE` could report the table as being corrupt. (Bug #26325)
- If an operation had an `InnoDB` table, and two triggers, `AFTER UPDATE` and `AFTER INSERT`, competing for different resources (such as two distinct `MyISAM` tables), the triggers were unable to execute concurrently. In addition, `INSERT` and `UPDATE` statements for the `InnoDB` table were unable to run concurrently. (Bug #26141)
- `ALTER DATABASE` did not require at least one option. (Bug #25859)
- Using `HANDLER` to open a table having a storage engine not supported by `HANDLER` properly returned an error, but also improperly prevented the table from being dropped by other connections. (Bug #25856)
- When using a `FEDERATED` table, the value of `LAST_INSERT_ID()` would not correctly update the C API interface, which would affect the autogenerated ID returned both through the C API and the MySQL protocol, affecting Connectors that used the protocol or C API. (Bug #25714)
- The server was blocked from opening other tables while the `FEDERATED` engine was attempting to open a remote table. Now the server does not check the correctness of a `FEDERATED` table at `CREATE TABLE` time, but waits until the table actually is accessed. (Bug #25679)
- Several `InnoDB` assertion failures were corrected. (Bug #25645)
- In a stored function or trigger, when `InnoDB` detected deadlock, it attempted rollback and displayed an incorrect error message (`Explicit or implicit commit is not permitted in stored function or trigger`). Now `InnoDB` returns an error under these conditions and does not attempt rollback. Rollback is handled outside of `InnoDB` above the function/trigger level. (Bug #24989)
- Dropping a temporary `InnoDB` table that had been locked with `LOCK TABLES` caused a server crash. (Bug #24918)
- On Windows, executables did not include Vista manifests. (Bug #24732)
References: See also: Bug #22563.
- If MySQL/`InnoDB` crashed very quickly after starting up, it would not force a checkpoint. In this case, `InnoDB` would skip crash recovery at next startup, and the database would become corrupt. Now, if the redo log scan at `InnoDB` startup goes past the last checkpoint, crash recovery is forced. (Bug #23710)
- `SHOW INNODB STATUS` caused an assertion failure under high load. (Bug #22819)
- A statement of the form `CREATE TABLE IF NOT EXISTS t1 SELECT f1() AS i` failed with a deadlock error if the stored function `f1()` referred to a table with the same name as the to-be-created table. Now it correctly produces a message that the table already exists. (Bug #22427)

- Read lock requests that were blocked by a pending write lock request were not permitted to proceed if the statement requesting the write lock was killed. (Bug #21281)
- On Windows, the server used 10MB of memory for each connection thread, resulting in memory exhaustion. Now each thread uses 1MB. (Bug #20815)
- InnoDB produced an unnecessary (and harmless) warning: `InnoDB: Error: trying to declare trx to enter InnoDB, but InnoDB: it already is declared.` (Bug #20090)
- `SQL_BIG_RESULT` had no effect for `CREATE TABLE ... SELECT SQL_BIG_RESULT ...` statements. (Bug #15130)
- `mysql_setpermission` tried to grant global-only privileges at the database level. (Bug #14618)
- For the general query log, logging of prepared statements executed using the C API differed from logging of prepared statements performed with `PREPARE` and `EXECUTE`. Logging for the latter was missing the `Prepare` and `Execute` lines. (Bug #13326)
- Backup software can cause `ERROR_SHARING_VIOLATION` or `ERROR_LOCK_VIOLATION` conditions during file operations. InnoDB now retries forever until the condition goes away. (Bug #9709)

Changes in MySQL Enterprise 5.0.46 [MRU] (2007-07-13)

This is a *Monthly Rapid Update* release of the MySQL Enterprise Server 5.0.

This section documents all changes and bugfixes that have been applied since the last MySQL Enterprise Server release (5.0.44). If you would like to receive more fine-grained and personalized *update alerts* about fixes that are relevant to the version and features you use, please consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details please see <http://www.mysql.com/products/enterprise/advisors.html>.

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- **MySQL Cluster:** `auto_increment_increment` and `auto_increment_offset` are now supported for NDB tables. (Bug #26342)
- **Replication:** The `sql_mode`, `foreign_key_checks`, `unique_checks`, character set/collations, and `sql_auto_is_null` session variables are written to the binary log and honored during replication. See [The Binary Log](#).
- If a `MERGE` table cannot be opened or used because of a problem with an underlying table, `CHECK TABLE` now displays information about which table caused the problem. (Bug #26976)

Bugs Fixed

- **MySQL Cluster:** When restarting a data node, queries could hang during that node's start phase 5, and continue only after the node had entered phase 6. (Bug #29364)
- **MySQL Cluster:** Replica redo logs were inconsistently handled during a system restart. (Bug #29354)
- **MySQL Cluster:** The management client's response to `START BACKUP WAIT COMPLETED` did not include the backup ID. (Bug #27640)
- **Replication:** `DROP USER` statements that named multiple users, only some of which could be dropped, were replicated incorrectly. (Bug #29030)

- On the IBM i5 platform, the installation script in the `.savf` binaries unconditionally executed the `mysql_install_db` script. (Bug #30084)
- `gcov` coverage-testing information was not written if the server crashed. (Bug #29543)
- Corrupt data resulted from use of `SELECT ... INTO OUTFILE 'file_name' FIELDS ENCLOSED BY 'c'`, where `c` is a digit or minus sign, followed by `LOAD DATA INFILE 'file_name' FIELDS ENCLOSED BY 'c'`. (Bug #29442)
- Use of `SHOW BINLOG EVENTS` for a nonexistent log file followed by `PURGE BINARY LOGS` caused a server crash. (Bug #29420)
- Assertion failure could occur for grouping queries that employed `DECIMAL` user variables with assignments to them. (Bug #29417)
- For `CAST(expr AS DECIMAL(M,D))`, the limits of 65 and 30 on the precision (`M`) and scale (`D`) were not enforced. (Bug #29415)
- Results for a select query that aliases the column names against a view could duplicate one column while omitting another. This bug could occur for a query over a multiple-table view that includes an `ORDER BY` clause in its definition. (Bug #29392)
- `mysqldump` created a stray file when a given a too-long file name argument. (Bug #29361)
- `FULLTEXT` indexes could be corrupted by certain `gbk` characters. (Bug #29299)
- `SELECT ... INTO OUTFILE` followed by `LOAD DATA` could result in garbled characters when the `FIELDS ENCLOSED BY` clause named a delimiter of `'0'`, `'b'`, `'n'`, `'r'`, `'t'`, `'N'`, or `'Z'` due to an interaction of character encoding and doubling for data values containing the enclosed-by character. (Bug #29294)
- Sort order of the collation wasn't used when comparing trailing spaces. This could lead to incorrect comparison results, incorrectly created indexes, or incorrect result set order for queries that include an `ORDER BY` clause. (Bug #29261)
- If an `ENUM` column contained `'` as one of its members (represented with numeric value greater than 0), and the column contained error values (represented as 0 and displayed as `'`), using `ALTER TABLE` to modify the column definition caused the 0 values to be given the numeric value of the nonzero `'` member. (Bug #29251)
- Calling `mysql_options()` after `mysql_real_connect()` could cause clients to crash. (Bug #29247)
- `CHECK TABLE` for `ARCHIVE` tables could falsely report table corruption or cause a server crash. (Bug #29207)
- Mixing binary and `utf8` columns in a union caused field lengths to be calculated incorrectly, resulting in truncation. (Bug #29205)
- `AsText()` could fail with a buffer overrun. (Bug #29166)
- `LOCK TABLES` was not atomic when more than one `InnoDB` tables were locked. (Bug #29154)
- A network structure was initialized incorrectly, leading to embedded server crashes. (Bug #29117)
- An assertion failure occurred if a query contained a conjunctive predicate of the form `view_column = constant` in the `WHERE` clause and the `GROUP BY` clause contained a reference to a different view column. The fix also enables application of an optimization that was being skipped if a query contained a conjunctive predicate of the form `view_column = constant` in the `WHERE` clause and the `GROUP BY` clause contained a reference to the same view column. (Bug #29104)

- If an `INSERT INTO ... SELECT` statement inserted into the same table that the `SELECT` retrieved from, and the `SELECT` included `ORDER BY` and `LIMIT` clauses, different data was inserted than the data produced by the `SELECT` executed by itself. (Bug #29095)
- Queries that performed a lookup into a `BINARY` index containing key values ending with spaces caused an assertion failure for debug builds and incorrect results for nondebug builds. (Bug #29087)
- The semantics of `BIGINT` depended on platform-specific characteristics. (Bug #29079)
- If one of the queries in a `UNION` used the `SQL_CACHE` option and another query in the `UNION` contained a nondeterministic function, the result was still cached. For example, this query was incorrectly cached:

```
SELECT NOW() FROM t1 UNION SELECT SQL_CACHE 1 FROM t1;
```

(Bug #29053)

- `REPLACE`, `INSERT IGNORE`, and `UPDATE IGNORE` did not work for `FEDERATED` tables. (Bug #29019)
- Inserting into `InnoDB` tables and executing `RESET MASTER` in multiple threads cause assertion failure in debug server binaries. (Bug #28983)
- For a `ucs2` column, `GROUP_CONCAT()` did not convert separators to the result character set before inserting them, producing a result containing a mixture of two different character sets. (Bug #28925)
- Queries using UDFs or stored functions were cached. (Bug #28921)
- For a join with `GROUP BY` or `ORDER BY` and a view reference in the `FROM` list, the query metadata erroneously showed empty table aliases and database names for the view columns. (Bug #28898)
- Non-`utf8` characters could get mangled when stored in `CSV` tables. (Bug #28862)
- `ALTER VIEW` is not supported as a prepared statement but was not being rejected. `ALTER VIEW` is now prohibited as a prepared statement or when called within stored routines. (Bug #28846)
- In strict SQL mode, errors silently stopped the SQL thread even for errors named using the `--slave-skip-errors` option. (Bug #28839)
- Runtime changes to the `log_queries_not_using_indexes` system variable were ignored. (Bug #28808)
- Selecting a column not present in the selected-from table caused an extra error to be produced by `SHOW ERRORS`. (Bug #28677)
- For a statement of the form `CREATE t1 SELECT integer_constant`, the server created the column using the `DECIMAL` data type for large negative values that are within the range of `BIGINT`. (Bug #28625)
- When one thread attempts to lock two (or more) tables and another thread executes a statement that aborts these locks (such as `REPAIR TABLE`, `OPTIMIZE TABLE`, or `CHECK TABLE`), the thread might get a table object with an incorrect lock type in the table cache. The result is table corruption or a server crash. (Bug #28574)
- `mysqlbinlog --hexdump` generated incorrect output due to omission of the “#” comment character for some comment lines. (Bug #28293)
- The `LOCATE()` function returned `NULL` if any of its arguments evaluated to `NULL`. Likewise, the predicate, `LOCATE(str, NULL) IS NULL`, erroneously evaluated to `FALSE`. (Bug #27932)

- The modification of a table by a partially completed multi-column update was not recorded in the binlog, rather than being marked by an event and a corresponding error code. (Bug #27716)
- A stack overrun could occur when storing `DATETIME` values using repeated prepared statements. (Bug #27592)
- Dropping a user-defined function could cause a server crash if the function was still in use by another thread. (Bug #27564)
- Unsafe aliasing in the source caused a client library crash when compiled with `gcc 4` at high optimization levels. (Bug #27383)
- Index-based range reads could fail for comparisons that involved contraction characters (such as `ch` in Czech or `ll` in Spanish). (Bug #27345)
- Aggregations in subqueries that refer to outer query columns were not always correctly referenced to the proper outer query. (Bug #27333)
- Error returns from the `time()` system call were ignored. (Bug #27198)
- Phantom reads could occur under `InnoDB SERIALIZABLE` isolation level. (Bug #27197)
- The `SUBSTRING()` function returned the entire string instead of an empty string when it was called from a stored procedure and when the length parameter was specified by a variable with the value "0". (Bug #27130)
- `ALTER TABLE ... ENABLE KEYS` could cause `mysqld` to crash when executed on a table containing on a `MyISAM` table containing billions of rows. (Bug #27029)
- Binary content `0x00` in a `BLOB` column sometimes became `0x5C 0x00` following a dump and reload, which could cause problems with data using multibyte character sets such as `GBK` (Chinese). This was due to a problem with `SELECT INTO OUTFILE` whereby `LOAD DATA` later incorrectly interpreted `0x5C` as the second byte of a multibyte sequence rather than as the `SOLIDUS` ("`\`") character, used by MySQL as the escape character. (Bug #26711)
- Index creation could corrupt the table definition in the `.frm` file: 1) A table with the maximum number of key segments and maximum length key name would have a corrupted `.frm` file, due to incorrect calculation of the total key length. 2) `MyISAM` would reject a table with the maximum number of keys and the maximum number of key segments in all keys. (It would permit one less than this total maximum.) Now `MyISAM` accepts a table defined with the maximum. (Bug #26642)
- The index merge union access algorithm could produce incorrect results with `InnoDB` tables. The problem could also occur for queries that used `DISTINCT`. (Bug #25798)
- Under ActiveState Perl, `mysql-test-run.pl` could kill itself when attempting to kill other processes. (Bug #25657)
- A query with `DISTINCT` in the select list to which the loose-scan optimization for grouping queries was applied returned an incorrect result set when the query was used with the `SQL_BIG_RESULT` option. (Bug #25602)
- For a multiple-row insert into a `FEDERATED` table that refers to a remote transactional table, if the insert failed for a row due to constraint failure, the remote table would contain a partial commit (the rows preceding the failed one) instead of rolling back the statement completely. This occurred because the rows were treated as individual inserts.

Now `FEDERATED` performs bulk-insert handling such that multiple rows are sent to the remote table in a batch. This provides a performance improvement and enables the remote table to perform statement rollback properly should an error occur. This capability has the following limitations:

- The size of the insert cannot exceed the maximum packet size between servers. If the insert exceeds this size, it is broken into multiple packets and the rollback problem can occur.
- Bulk-insert handling does not occur for `INSERT ... ON DUPLICATE KEY UPDATE`.

(Bug #25513)

- The `FEDERATED` storage engine failed silently for `INSERT ... ON DUPLICATE KEY UPDATE` if a duplicate key violation occurred. `FEDERATED` does not support `ON DUPLICATE KEY UPDATE`, so now it correctly returns an `ER_DUP_KEY` error if a duplicate key violation occurs. (Bug #25511)
- A too-long `shared-memory-base-name` value could cause a buffer overflow and crash the server or clients. (Bug #24924)
- The server deducted some bytes from the `key_cache_block_size` option value and reduced it to the next lower 512 byte boundary. The resulting block size was not a power of two. Setting the `key_cache_block_size` system variable to a value that is not a power of two resulted in `MyISAM` table corruption. (Bug #23068, Bug #28478, Bug #25853)
- `SHOW BINLOG EVENTS` displayed incorrect values of `End_log_pos` for events associated with transactional storage engines. (Bug #22540)
- Under ActiveState Perl, `mysql-test-run.pl` would not run. (Bug #18415)
- The server crashed when the size of an `ARCHIVE` table grew larger than 2GB. (Bug #15787)
- On 64-bit Windows systems, the Config Wizard failed to complete the setup because 64-bit Windows does not resolve dynamic linking of the 64-bit `libmysql.dll` to a 32-bit application like the Config Wizard. (Bug #14649)
- The server returned data from `SHOW CREATE TABLE` statement or a `SELECT` statement on an `INFORMATION_SCHEMA` table using the `binary` character set. (Bug #10491)

Changes in MySQL Community Server 5.0.45 (2007-07-04)

This is a bugfix release for the current MySQL Community Server production release family. It replaces MySQL 5.0.41.

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- **Incompatible Change:** Prior to this release, when `DATE` values were compared with `DATETIME` values, the time portion of the `DATETIME` value was ignored, or the comparison could be performed as a string compare. Now a `DATE` value is coerced to the `DATETIME` type by adding the time portion as `00:00:00`. To mimic the old behavior, use the `CAST()` function as shown in this example: `SELECT date_col = CAST(NOW() AS DATE) FROM table;` (Bug #28929)
- **Incompatible Change:** `INSERT DELAYED` is now downgraded to a normal `INSERT` if the statement uses functions that access tables or triggers, or that is called from a function or a trigger.

This was done to resolve the following interrelated issues:

- The server could abort or deadlock for `INSERT DELAYED` statements for which another insert was performed implicitly (for example, using a stored function that inserted a row).

- A trigger using an `INSERT DELAYED` caused the error `INSERT DELAYED can't be used with table ... because it is locked with LOCK TABLES` although the target table was not actually locked.
- `INSERT DELAYED` into a table with a `BEFORE INSERT` or `AFTER INSERT` trigger gave an incorrect `NEW` pseudocolumn value and caused the server to deadlock or abort.

(Bug #21483)

References: See also: Bug #20497, Bug #21714.

- **MySQL Cluster:** The server source tree now includes scripts to simplify building MySQL with SCI support. For more information about SCI interconnects and these build scripts, see [Configuring MySQL Cluster to use SCI Sockets](#). (Bug #25470)
- Binaries for the Linux x86 statically linked `tar.gz` Community package were linked dynamically, not statically. Static linking has been re-enabled. (Bug #29617)
- `INSERT DELAYED` statements on `BLACKHOLE` tables are now rejected, due to the fact that the `BLACKHOLE` storage engine does not support them. (Bug #27998)
- A new status variable, `Com_call_procedure`, indicates the number of calls to stored procedures. (Bug #27994)
- Potential memory leaks in `SHOW PROFILE` were eliminated. (Bug #24795)

Bugs Fixed

- **Security Fix:** A malformed password packet in the connection protocol could cause the server to crash. Thanks for Dormando for reporting this bug, and for providing details and a proof of concept. (Bug #28984, CVE-2007-3780)
- **Security Fix:** Use of a view could enable a user to gain update privileges for tables in other databases. (Bug #27878, CVE-2007-3782)
- **Security Fix:** The requirement of the `DROP` privilege for `RENAME TABLE` was not enforced. (Bug #27515, CVE-2007-2691)
- **Security Fix:** If a stored routine was declared using `SQL SECURITY INVOKER`, a user who invoked the routine could gain privileges. (Bug #27337, CVE-2007-2692)
- **Security Fix:** `CREATE TABLE LIKE` did not require any privileges on the source table. Now it requires the `SELECT` privilege.

In addition, `CREATE TABLE LIKE` was not isolated from alteration by other connections, which resulted in various errors and incorrect binary log order when trying to execute concurrently a `CREATE TABLE LIKE` statement and either DDL statements on the source table or DML or DDL statements on the target table. (Bug #23667, Bug #25578, CVE-2007-3781)

- **Incompatible Change:** The names of stored functions referenced by views were not properly displayed by `SHOW CREATE VIEW`.

The fix corrects a problem introduced by Bug #23491. There is an incompatibility when upgrading from versions affected by that bug fix (MySQL 5.0.40 through 5.0.43, MySQL 5.1.18 through 5.1.19): If you use `mysqldump` before upgrading from an affected version and reload the data after upgrading to a higher version, you must drop and recreate your views. (Bug #28605)

References: This issue is a regression of: Bug #23491.

- **Incompatible Change:** When `mysqldump` was run with the `--delete-master-logs` option, binary log files were deleted before it was known that the dump had succeeded, not after. (The method for removing log files used `RESET MASTER` prior to the dump. This also reset the binary log sequence numbering to `.000001`.) Now `mysqldump` flushes the logs (which creates a new binary log number with the next sequence number), performs the dump, and then uses `PURGE BINARY LOGS` to remove the log files older than the new one. This also preserves log numbering because the new log with the next number is generated and only the preceding logs are removed. However, this may affect applications if they rely on the log numbering sequence being reset. (Bug #24733)
- **Incompatible Change:** The use of an `ORDER BY` or `DISTINCT` clause with a query containing a call to the `GROUP_CONCAT()` function caused results from previous queries to be redisplayed in the current result. The fix for this includes replacing a `BLOB` value used internally for sorting with a `VARCHAR`. This means that for long results (more than 65,535 bytes), it is possible for truncation to occur; if so, an appropriate warning is issued. (Bug #23856, Bug #28273)
- **MySQL Cluster:** A corrupt schema file could cause a `File already open` error. (Bug #28770)
- **MySQL Cluster:** `UPDATE IGNORE` statements involving the primary keys of multiple tables could result in data corruption. (Bug #28719)
- **MySQL Cluster:** A race condition could result when nonmaster nodes (in addition to the master node) tried to update active status due to a local checkpoint (that is, between `NODE_FAILREP` and `COPY_GCIREQ` events). Now only the master updates the active status. (Bug #28717)
- **MySQL Cluster:** A fast global checkpoint under high load with high usage of the redo buffer caused data nodes to fail. (Bug #28653)
- **MySQL Cluster:** When an API node sent more than 1024 signals in a single batch, `NDB` would process only the first 1024 of these, and then hang. (Bug #28443)
- **MySQL Cluster:** A delay in obtaining `AUTO_INCREMENT` IDs could lead to excess temporary errors. (Bug #28410)
- **MySQL Cluster:** The cluster waited 30 seconds instead of 30 milliseconds before reading table statistics. (Bug #28093)
- **MySQL Cluster:** `INSERT IGNORE` wrongly ignored `NULL` values in unique indexes. (Bug #27980)
- **MySQL Cluster:** The name of the month "March" was given incorrectly in the cluster error log. (Bug #27926)
- **MySQL Cluster:** It was not possible to add a unique index to an `NDB` table while in single user mode. (Bug #27710)
- **MySQL Cluster:** Repeated insertion of data generated by `mysqldump` into `NDB` tables could eventually lead to failure of the cluster. (Bug #27437)
- **MySQL Cluster:** `ndb_connectstring` did not appear in the output of `SHOW VARIABLES`. (Bug #26675)
- **MySQL Cluster:** A failure to release internal resources following an error could lead to problems with single user mode. (Bug #25818)
- **Replication:** The result of executing of a prepared statement created with `PREPARE s FROM "SELECT 1 LIMIT ?"` was not replicated correctly. (Bug #28464)
- **Replication:** Recreating a view that already exists on the master would cause a replicating slave to terminate replication with a 'different error message on slave and master' error. (Bug #28244)

- **Replication:** Binary logging of prepared statements could produce syntactically incorrect queries in the binary log, replacing some parameters with variable names rather than variable values. This could lead to incorrect results on replication slaves. (Bug #26842, Bug #12826)
- **Replication:** Connections from one `mysqld` server to another failed on Mac OS X, affecting replication and `FEDERATED` tables. (Bug #26664)

References: See also: Bug #29083.

- **Replication:** Aborting a statement on the master that applied to a nontransactional statement broke replication. The statement was written to the binary log but not completely executed on the master. Slaves receiving the statement executed it completely, resulting in loss of data synchrony. Now an error code is written to the error log so that the slaves stop without executing the aborted statement. (That is, replication stops, but synchrony to the point of the stop is preserved and you can investigate the problem.) (Bug #26551)
- **Replication:** Restoration of the default database after stored routine or trigger execution on a slave could cause replication to stop if the database no longer existed. (Bug #25082)
- **Replication:** When using transactions and replication, shutting down the master in the middle of a transaction would cause all slaves to stop replicating. (Bug #22725)
- **Replication:** Using `CREATE TABLE LIKE ...` would raise an assertion when replicated to a slave. (Bug #18950)
- **Cluster API:** For `BLOB` reads on operations with lock mode `LM_CommittedRead`, the lock mode was not upgraded to `LM_Read` before the state of the `BLOB` had already been calculated. The `NDB` API methods affected by this problem included the following:
 - `NdbOperation::readTuple()`
 - `NdbScanOperation::readTuples()`
 - `NdbIndexScanOperation::readTuples()`(Bug #27320)
- On the IBM i5 platform, the installation script in the `.savf` binaries unconditionally executed the `mysql_install_db` script. This problem was fixed in a repackaged distribution numbered 5.0.45b. (Bug #30084)
- Long path names for internal temporary tables could cause stack overflows. (Bug #29015)
- Using an `INTEGER` column from a table to `ROUND()` a number produced different results than using a constant with the same value as the `INTEGER` column. (Bug #28980)
- If a program binds a given number of parameters to a prepared statement handle and then somehow changes `stmt->param_count` to a different number, `mysql_stmt_execute()` could crash the client or server. (Bug #28934)
- `INSERT .. ON DUPLICATE KEY UPDATE` could under some circumstances silently update rows when it should not have. (Bug #28904)
- Queries that used `UUID()` were incorrectly permitted into the query cache. (This should not happen because `UUID()` is nondeterministic.) (Bug #28897)
- Using a `VIEW` created with a nonexisting `DEFINER` could lead to incorrect results under some circumstances. (Bug #28895)

- On Windows, `USE_TLS` was not defined for `mysqlclient.lib`. (Bug #28860)
- A subquery with `ORDER BY` and `LIMIT 1` could cause a server crash. (Bug #28811)
- Using `BETWEEN` with nonindexed date columns and short formats of the date string could return incorrect results. (Bug #28778)
- Selecting `GEOMETRY` columns in a `UNION` caused a server crash. (Bug #28763)
- When constructing the path to the original `.frm` file, `ALTER ... RENAME` was unnecessarily (and incorrectly) lowercasing the entire path when not on a case-insensitive file system, causing the statement to fail. (Bug #28754)
- Searches on indexed and nonindexed `ENUM` columns could return different results for empty strings. (Bug #28729)
- Executing `EXPLAIN EXTENDED` on a query using a derived table over a grouping subselect could lead to a server crash. This occurred only when materialization of the derived tables required creation of an auxiliary temporary table, an example being when a grouping operation was carried out with usage of a temporary table. (Bug #28728)
- The result of evaluation for a view's `CHECK OPTION` option over an updated record and records of merged tables was arbitrary and dependent on the order of records in the merged tables during the execution of the `SELECT` statement. (Bug #28716)
- The “manager thread” of the LinuxThreads implementation was unintentionally started before `mysqld` had dropped privileges (to run as an unprivileged user). This caused signaling between threads in `mysqld` to fail when the privileges were finally dropped. (Bug #28690)
- For debug builds, `ALTER TABLE` could trigger an assertion failure due to occurrence of a deadlock when committing changes. (Bug #28652)
- Killing from one connection a long-running `EXPLAIN QUERY` started from another connection caused `mysqld` to crash. (Bug #28598)
- Outer join queries with `ON` conditions over constant outer tables did not return `NULL`-complemented rows when conditions were evaluated to `FALSE`. (Bug #28571)
- An update on a multiple-table view with the `CHECK OPTION` clause and a subquery in the `WHERE` condition could cause an assertion failure. (Bug #28561)
- `PURGE MASTER LOGS BEFORE (subquery)` caused a server crash. Subqueries are forbidden in the `BEFORE` clause now. (Bug #28553)
- `mysqldump` calculated the required memory for a hex-blob string incorrectly causing a buffer overrun. This in turn caused `mysqldump` to crash silently and produce incomplete output. (Bug #28522)
- Passing a `DECIMAL` value as a parameter of a statement prepared with `PREPARE` resulted in an error. (Bug #28509)
- `mysql_affected_rows()` could return an incorrect result for `INSERT ... ON DUPLICATE KEY UPDATE` if the `CLIENT_FOUND_ROWS` flag was set. (Bug #28505)
- A query that grouped by the result of an expression returned a different result when the expression was assigned to a user variable. (Bug #28494)
- Subselects returning `LONG` values in MySQL versions later than 5.0.24a returned `LONGLONG` prior to this. The previous behavior was restored. (Bug #28492)

References: This issue is a regression of: Bug #19714.

- Forcing the use of an index on a `SELECT` query when the index had been disabled would raise an error without running the query. The query now executes, with a warning generated noting that the use of a disabled index has been ignored. (Bug #28476)
- The query `SELECT '2007-01-01' + INTERVAL column_name DAY FROM table_name` caused `mysqld` to fail. (Bug #28450)
- A server crash could happen under rare conditions such that a temporary table outgrew heap memory reserved for it and the remaining disk space was not big enough to store the table as a `MyISAM` table. (Bug #28449)
- `mysql_upgrade` failed if certain SQL modes were set. Now it sets the mode itself to avoid this problem. (Bug #28401)
- A query with a `NOT IN` subquery predicate could cause a crash when the left operand of the predicate evaluated to `NULL`. (Bug #28375)
- The test case for `mysqldump` failed with `bin-log` disabled. (Bug #28372)
- Attempting to `LOAD_FILE` from an empty floppy drive under Windows, caused the server to hang. For example, if you opened a connection to the server and then issued the command `SELECT LOAD_FILE('a:test');`, with no floppy in the drive, the server was inaccessible until the modal pop-up dialog box was dismissed. (Bug #28366)
- A buffer overflow could occur when using `DECIMAL` columns on Windows operating systems. (Bug #28361)
- `libmysql.dll` could not be dynamically loaded on Windows. (Bug #28358)
- Grouping queries with correlated subqueries in `WHERE` conditions could produce incorrect results. (Bug #28337)
- `mysqltest` used a too-large stack size on PowerPC/Debian Linux, causing thread-creation failure for tests that use many threads. (Bug #28333)
- `EXPLAIN` for a query on an empty table immediately after its creation could result in a server crash. (Bug #28272)
- The `IS_UPDATABLE` column in the `INFORMATION_SCHEMA.VIEWS` table was not always set correctly. (Bug #28266)
- Comparing a `DATETIME` column value with a user variable yielded incorrect results. (Bug #28261)
- For `CAST()` of a `NULL` value with type `DECIMAL`, the return value was incorrectly initialized, producing a runtime error for binaries built using Visual C++ 2005. (Bug #28250)
- Portability problems caused by use of `isinf()` were corrected. (Bug #28240)
- When dumping procedures, `mysqldump --compact` generated output that restored the session variable `sql_mode` without first capturing it. When dumping routines, `mysqldump --compact` neither set nor retrieved the value of `sql_mode`. (Bug #28223)
- Comparison of the string value of a date showed as unequal to `CURTIME()`. Similar behavior was exhibited for `DATETIME` values. (Bug #28208)
- For `InnoDB`, in some rare cases the optimizer preferred a more expensive `ref` access to a less expensive range access. (Bug #28189)
- A performance degradation was observed for outer join queries to which a not-exists optimization was applied. (Bug #28188)

- `SELECT * INTO OUTFILE ... FROM INFORMATION_SCHEMA.SCHEMATA` failed with an `Access denied` error, even for a user who had the `FILE` privilege. (Bug #28181)
- The `Bytes_received` and `Bytes_sent` status variables could hold only 32-bit values (not 64-bit values) on some platforms. (Bug #28149)
- Comparisons of `DATE` or `DATETIME` values for the `IN()` function could yield incorrect results. (Bug #28133)
- Storing a large number into a `FLOAT` or `DOUBLE` column with a fixed length could result in incorrect truncation of the number if the column's length was greater than 31. (Bug #28121)
- The server could hang for `INSERT IGNORE ... ON DUPLICATE KEY UPDATE` if an update failed. (Bug #28000)
- `DECIMAL` values beginning with nine 9 digits could be incorrectly rounded. (Bug #27984)
- `CAST()` to `DECIMAL` did not check for overflow. (Bug #27957)
- For `INSERT ... ON DUPLICATE KEY UPDATE` statements that affected many rows, updates could be applied to the wrong rows. (Bug #27954)
- Early `NULL`-filtering optimization did not work for `eq_ref` table access. (Bug #27939)
- The second execution of a prepared statement from a `UNION` query with `ORDER BY RAND()` caused the server to crash. This problem could also occur when invoking a stored procedure containing such a query. (Bug #27937)
- Views ignored precision for `CAST()` operations. (Bug #27921)
- For attempts to open a nonexistent table, the server should report `ER_NO_SUCH_TABLE` but sometimes reported `ER_TABLE_NOT_LOCKED`. (Bug #27907)
- A stored program that uses a variable name containing multibyte characters could fail to execute. (Bug #27876)
- Nongrouped columns were permitted by `*` in `ONLY_FULL_GROUP_BY` SQL mode. (Bug #27874)
- `ON` conditions from `JOIN` expressions were ignored when checking the `CHECK OPTION` clause while updating a multiple-table view that included such a clause. (Bug #27827)
- Debug builds on Windows generated false alarms about uninitialized variables with some Visual Studio runtime libraries. (Bug #27811)
- Certain queries that used uncorrelated scalar subqueries caused `EXPLAIN` to crash. (Bug #27807)
- Changes to some system variables should invalidate statements in the query cache, but invalidation did not happen. (Bug #27792)
- Performing a `UNION` on two views that had `ORDER BY` clauses resulted in an `Unknown column` error. (Bug #27786)
- `mysql_install_db` is supposed to detect existing system tables and create only those that do not exist. Instead, it was exiting with an error if tables already existed. (Bug #27783)
- On some systems, `udf_example.c` returned an incorrect result length. Also on some systems, `mysql-test-run.pl` could not find the shared object built from `udf_example.c`. (Bug #27741)
- `mysqld` did not check the length of option values and could crash with a buffer overflow for long values. (Bug #27715)

- Comparisons using row constructors could fail for rows containing `NULL` values. (Bug #27704)
- `LOAD DATA` did not use `CURRENT_TIMESTAMP` as the default value for a `TIMESTAMP` column for which no value was provided. (Bug #27670)
- `mysqldump` could not connect using SSL. (Bug #27669)
- On Linux, the server could not create temporary tables if `lower_case_table_names` was set to 1 and the value of `tmpdir` was a directory name containing any uppercase letters. (Bug #27653)
- For InnoDB tables, a multiple-row `INSERT` of the form `INSERT INTO t (id...) VALUES (NULL...) ON DUPLICATE KEY UPDATE id=VALUES(id)`, where `id` is an `AUTO_INCREMENT` column, could cause `ERROR 1062 (23000): Duplicate entry...` errors or lost rows. (Bug #27650)
- `HASH` indexes on `VARCHAR` columns with binary collations did not ignore trailing spaces from strings before comparisons. This could result in duplicate records being successfully inserted into a `MEMORY` table with unique key constraints. A consequence was that internal `MEMORY` tables used for `GROUP BY` calculation contained duplicate rows that resulted in duplicate-key errors when converting those temporary tables to `MyISAM`, and that error was incorrectly reported as a `table is full` error. (Bug #27643)
- The XML output representing an empty result was an empty string rather than an empty `<resultset/>` element. (Bug #27608)
- An error occurred trying to connect to `mysqld-debug.exe`. (Bug #27597)
- Comparison of a `DATE` with a `DATETIME` did not treat the `DATE` as having a time part of `00:00:00`. (Bug #27590)

References: See also: Bug #32198.

- Selecting `MIN()` on an indexed column that contained only `NULL` values caused `NULL` to be returned for other result columns. (Bug #27573)
- If a stored function or trigger was killed, it aborted but no error was thrown, permitting the calling statement to continue without noticing the problem. This could lead to incorrect results. (Bug #27563)
- The fix for Bug #17212 provided correct sort order for misordered output of certain queries, but caused significant overall query performance degradation. (Results were correct (good), but returned much more slowly (bad).) The fix also affected performance of queries for which results were correct. The performance degradation has been addressed. (Bug #27531)

References: This issue is a regression of: Bug #17212.

- The `CRC32()` function returns an unsigned integer, but the metadata was signed, which could cause certain queries to return incorrect results. (For example, queries that selected a `CRC32()` value and used that value in the `GROUP BY` clause.) (Bug #27530)
- An interaction between `SHOW TABLE STATUS` and other concurrent statements that modify the table could result in a divide-by-zero error and a server crash. (Bug #27516)
- When `ALTER TABLE` was used to add a new `DATE` column with no explicit default value, `'0000-00-00'` was used as the default even if the SQL mode included the `NO_ZERO_DATE` mode to prohibit that value. A similar problem occurred for `DATETIME` columns. (Bug #27507)
- A race condition between `DROP TABLE` and `SHOW TABLE STATUS` could cause the latter to display incorrect information. (Bug #27499)

- Using a `TEXT` local variable in a stored routine in an expression such as `SET var = SUBSTRING(var, 3)` produced an incorrect result. (Bug #27415)
- Nested aggregate functions could be improperly evaluated. (Bug #27363)
- A stored function invocation in the `WHERE` clause was treated as a constant. (Bug #27354)
- Failure to allocate memory associated with `transaction_prealloc_size` could cause a server crash. (Bug #27322)
- `mysqldump` crashed if it got no data from `SHOW CREATE PROCEDURE` (for example, when trying to dump a routine defined by a different user and for which the current user had no privileges). Now it prints a comment to indicate the problem. It also returns an error, or continues if the `--force` option is given. (Bug #27293)
- The error message for error number 137 did not report which database/table combination reported the problem. (Bug #27173)
- `mysqlbinlog` produced different output with the `-R` option than without it. (Bug #27171)
- A large filesort could result in a division by zero error and a server crash. (Bug #27119)
- Times displayed by `SHOW PROFILE` were incorrectly associated with the profile entry one later than the correct one. (Bug #27060)
- Flow control optimization in stored routines could cause exception handlers to never return or execute incorrect logic. (Bug #26977)
- `SHOW PROFILE` hung if executed before enabling the `@@profiling` session variable. (Bug #26938)
- `mysqldump` would not dump a view for which the `DEFINER` no longer exists. (Bug #26817)
- Creating a temporary table with `InnoDB` when using the one-file-per-table setting, and when the host file system for temporary tables was `tmpfs`, would cause an assertion within `mysqld`. This was due to the use of `O_DIRECT` when opening the temporary table file. (Bug #26662)
- `mysql_upgrade` did not detect failure of external commands that it runs. (Bug #26639)
- Some test suite files were missing from some MySQL-test packages. (Bug #26609)
- Statements within triggers ignored the value of the `low_priority_updates` system variable. (Bug #26162)

References: See also: Bug #29963.

- Index hints (`USE INDEX`, `IGNORE INDEX`, `FORCE INDEX`) cannot be used with `FULLTEXT` indexes, but were not being ignored. (Bug #25951)
- If `CREATE TABLE t1 LIKE t2` failed due to a full disk, an empty `t2.frm` file could be created but not removed. This file then caused subsequent attempts to create a table named `t2` to fail. This is easily corrected at the file system level by removing the `t2.frm` file manually, but now the server removes the file if the create operation does not complete successfully. (Bug #25761)
- Running `CHECK TABLE` concurrently with a `SELECT`, `INSERT` or other statement on Windows could corrupt a MyISAM table. (Bug #25712)
- On Windows, connection handlers did not properly decrement the server's thread count when exiting. (Bug #25621)
- `mysql_upgrade` did not pass a password to `mysqlcheck` if one was given. (Bug #25452)

- On Windows, `mysql_upgrade` was sensitive to lettercase of the names of some required components. (Bug #25405)
- For storage engines that permit the current auto-increment value to be set, using `ALTER TABLE ... ENGINE` to convert a table from one such storage engine to another caused loss of the current value. (For storage engines that do not support setting the value, it cannot be retained anyway when changing the storage engine.) (Bug #25262)
- Due to a race condition, executing `FLUSH PRIVILEGES` in one thread could cause brief table unavailability in other threads. (Bug #24988)
- Several math functions produced incorrect results for large unsigned values. `ROUND()` produced incorrect results or a crash for a large number-of-decimals argument. (Bug #24912)
- The result set of a query that used `WITH ROLLUP` and `DISTINCT` could lack some rollup rows (rows with `NULL` values for grouping attributes) if the `GROUP BY` list contained constant expressions. (Bug #24856)
- For queries that used `ORDER BY` with InnoDB tables, if the optimizer chose an index for accessing the table but found a covering index that enabled the `ORDER BY` to be skipped, no results were returned. (Bug #24778)
- Concurrent execution of `CREATE TABLE ... SELECT` and other statements involving the target table suffered from various race conditions, some of which might have led to deadlocks. (Bug #24738)
- On some Linux distributions where LinuxThreads and NPTL `glibc` versions both are available, statically built binaries can crash because the linker defaults to LinuxThreads when linking statically, but calls to external libraries (such as `libnss`) are resolved to NPTL versions. This cannot be worked around in the code, so instead if a crash occurs on such a binary/OS combination, print an error message that provides advice about how to fix the problem. (Bug #24611)
- An attempt to execute `CREATE TABLE ... SELECT` when a temporary table with the same name already existed led to the insertion of data into the temporary table and creation of an empty nontemporary table. (Bug #24508)
- The `MERGE` storage engine could return incorrect results when several index values that compare equality were present in an index (for example, `'gross'` and `'gross '`, which are considered equal but have different lengths). (Bug #24342)
- Some upgrade problems are detected and better error messages suggesting that `mysql_upgrade` be run are produced. (Bug #24248)
- Some views could not be created even when the user had the requisite privileges. (Bug #24040)
- Using `CAST()` to convert `DATETIME` values to numeric values did not work. (Bug #23656)
- The `AUTO_INCREMENT` value would not be correctly reported for InnoDB tables when using `SHOW CREATE TABLE` statement or `mysqldump` command. (Bug #23313)
- Implicit conversion of `9912101` to `DATE` did not match `CAST(9912101 AS DATE)`. (Bug #23093)
- Conversion errors could occur when constructing the condition for an `IN` predicate. The predicate was treated as if the affected column contains `NULL`, but if the `IN` predicate is inside `NOT`, incorrect results could be returned. (Bug #22855)
- `SELECT COUNT(*)` from a table containing a `DATETIME NOT NULL` column could produce spurious warnings with the `NO_ZERO_DATE` SQL mode enabled. (Bug #22824)

- Using `SET GLOBAL` to change the `lc_time_names` system variable had no effect on new connections. (Bug #22648)
- A multiple-table `UPDATE` could return an incorrect rows-matched value if, during insertion of rows into a temporary table, the table had to be converted from a `MEMORY` table to a `MyISAM` table. (Bug #22364)
- `yaSSL` crashed on pre-Pentium Intel CPUs. (Bug #21765)
- Linux binaries were unable to dump core after executing a `setuid()` call. (Bug #21723)
- A slave that used `--master-ssl-cipher` could not connect to the master. (Bug #21611)
- Quoted labels in stored routines were mishandled, rendering the routines unusable. (Bug #21513)
- Stack overflow caused server crashes. (Bug #21476)
- `CURDATE()` is less than `NOW()`, either when comparing `CURDATE()` directly (`CURDATE() < NOW()` is true) or when casting `CURDATE()` to `DATE` (`CAST(CURDATE() AS DATE) < NOW()` is true). However, storing `CURDATE()` in a `DATE` column and comparing `col_name < NOW()` incorrectly yielded false. This is fixed by comparing a `DATE` column as `DATETIME` for comparisons to a `DATETIME` constant. (Bug #21103)
- `CREATE TABLE IF NOT EXISTS ... SELECT` caused a server crash if the target table already existed and had a `BEFORE INSERT` trigger. (Bug #20903)
- Deadlock occurred for attempts to execute `CREATE TABLE IF NOT EXISTS ... SELECT` when `LOCK TABLES` had been used to acquire a read lock on the target table. (Bug #20662, Bug #15522)
- Changing a `utf8` column in an `InnoDB` table to a shorter length did not shorten the data values. (Bug #20095)
- For dates with 4-digit year parts less than 200, an incorrect implicit conversion to add a century was applied for date arithmetic performed with `DATE_ADD()`, `DATE_SUB()`, `+ INTERVAL`, and `- INTERVAL`. (For example, `DATE_ADD('0050-01-01 00:00:00', INTERVAL 0 SECOND)` became `'2050-01-01 00:00:00'`.) (Bug #18997)
- Granting access privileges to an individual table where the database or table name contained an underscore failed. (Bug #18660)
- The `-lmtmalloc` library was removed from the output of `mysql_config` on Solaris, as it caused problems when building `DBD::mysql` (and possibly other applications) on that platform that tried to use `dlopen()` to access the client library. (Bug #18322)
- The `check-cpu` script failed to detect AMD64 Turion processors correctly. (Bug #17707)
- Trying to shut down the server following a failed `LOAD DATA INFILE` caused `mysqld` to crash. (Bug #17233)
- The omission of leading zeros in dates could lead to erroneous results when these were compared with the output of certain date and time functions. (Bug #16377)
- `INSERT...ON DUPLICATE KEY UPDATE` could cause `Error 1032: Can't find record in ...` for inserts into an `InnoDB` table unique index using key column prefixes with an underlying `utf8` string column. (Bug #13191)
- Having the `EXECUTE` privilege for a routine in a database should make it possible to `USE` that database, but the server returned an error instead. This has been corrected. As a result of the change, `SHOW TABLES` for a database in which you have only the `EXECUTE` privilege returns an empty set rather than an error. (Bug #9504)

Changes in MySQL Enterprise 5.0.44sp1 [QSP] (2007-08-01)

This is a *Service Pack* release of the MySQL Enterprise Server 5.0.

This section documents all changes and bug fixes that have been applied since the last MySQL Enterprise Server release (5.0.44).

Bugs Fixed

- Using the `DATE()` function in a `WHERE` clause did not return any records after encountering `NULL`. However, using `TRIM()` or `CAST()` produced the correct results. (Bug #29898)
- For a table with a `DATE` column `date_col` such that selecting rows with `WHERE date_col = 'date_val 00:00:00'` yielded a nonempty result, adding `GROUP BY date_col` caused the result to be empty. (Bug #29729)
- Optimization of queries with `DETERMINISTIC` stored functions in the `WHERE` clause was ineffective: A sequential scan was always used. (Bug #29338)
- Creation of a legal stored procedure could fail if no default database had been selected. (Bug #29050)
- If a stored procedure was created and invoked prior to selecting a default database with `USE`, a `No database selected` error occurred. (Bug #28551)

Changes in MySQL Enterprise 5.0.44 [MRU] (2007-06-21)

This is a *Monthly Rapid Update* release of the MySQL Enterprise Server 5.0.

This section documents all changes and bug fixes that have been applied since the last MySQL Enterprise Server release (5.0.42).

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- **MySQL Cluster:** The server source tree now includes scripts to simplify building MySQL with SCI support. For more information about SCI interconnects and these build scripts, see [Configuring MySQL Cluster to use SCI Sockets](#). (Bug #25470)
- Enterprise builds did not include the `CSV` storage engine. `CSV` is now included in Enterprise builds for all platforms except Windows, QNX, and NetWare. (Bug #28844)
- `INSERT DELAYED` statements on `BLACKHOLE` tables are now rejected, due to the fact that the `BLACKHOLE` storage engine does not support them. (Bug #27998)
- A new status variable, `Com_call_procedure`, indicates the number of calls to stored procedures. (Bug #27994)

Bugs Fixed

- **Security Fix:** A malformed password packet in the connection protocol could cause the server to crash. Thanks for Dormando for reporting this bug, and for providing details and a proof of concept. (Bug #28984, CVE-2007-3780)
- **Security Fix:** `CREATE TABLE LIKE` did not require any privileges on the source table. Now it requires the `SELECT` privilege.

In addition, `CREATE TABLE LIKE` was not isolated from alteration by other connections, which resulted in various errors and incorrect binary log order when trying to execute concurrently a `CREATE TABLE LIKE` statement and either DDL statements on the source table or DML or DDL statements on the target table. (Bug #23667, Bug #25578, CVE-2007-3781)

- **Incompatible Change:** The names of stored functions referenced by views were not properly displayed by `SHOW CREATE VIEW`.

The fix corrects a problem introduced by Bug #23491. There is an incompatibility when upgrading from versions affected by that bug fix (MySQL 5.0.40 through 5.0.43, MySQL 5.1.18 through 5.1.19): If you use `mysqldump` before upgrading from an affected version and reload the data after upgrading to a higher version, you must drop and recreate your views. (Bug #28605)

References: This issue is a regression of: Bug #23491.

- **Incompatible Change:** When `mysqldump` was run with the `--delete-master-logs` option, binary log files were deleted before it was known that the dump had succeeded, not after. (The method for removing log files used `RESET MASTER` prior to the dump. This also reset the binary log sequence numbering to `.000001`.) Now `mysqldump` flushes the logs (which creates a new binary log number with the next sequence number), performs the dump, and then uses `PURGE BINARY LOGS` to remove the log files older than the new one. This also preserves log numbering because the new log with the next number is generated and only the preceding logs are removed. However, this may affect applications if they rely on the log numbering sequence being reset. (Bug #24733)
- **Incompatible Change:** The use of an `ORDER BY` or `DISTINCT` clause with a query containing a call to the `GROUP_CONCAT()` function caused results from previous queries to be redisplayed in the current result. The fix for this includes replacing a `BLOB` value used internally for sorting with a `VARCHAR`. This means that for long results (more than 65,535 bytes), it is possible for truncation to occur; if so, an appropriate warning is issued. (Bug #23856, Bug #28273)
- **MySQL Cluster:** A corrupt schema file could cause a `File already open` error. (Bug #28770)
- **MySQL Cluster:** `UPDATE IGNORE` statements involving the primary keys of multiple tables could result in data corruption. (Bug #28719)
- **MySQL Cluster:** A race condition could result when nonmaster nodes (in addition to the master node) tried to update active status due to a local checkpoint (that is, between `NODE_FAILREP` and `COPY_GCIREQ` events). Now only the master updates the active status. (Bug #28717)
- **MySQL Cluster:** A fast global checkpoint under high load with high usage of the redo buffer caused data nodes to fail. (Bug #28653)
- **MySQL Cluster:** When an API node sent more than 1024 signals in a single batch, `NDB` would process only the first 1024 of these, and then hang. (Bug #28443)
- **MySQL Cluster:** A delay in obtaining `AUTO_INCREMENT` IDs could lead to excess temporary errors. (Bug #28410)
- **MySQL Cluster:** A failure to release internal resources following an error could lead to problems with single user mode. (Bug #25818)
- **Replication:** The result of executing of a prepared statement created with `PREPARE s FROM "SELECT 1 LIMIT ?"` was not replicated correctly. (Bug #28464)
- **Replication:** Recreating a view that already exists on the master would cause a replicating slave to terminate replication with a 'different error message on slave and master' error. (Bug #28244)

- **Replication:** Binary logging of prepared statements could produce syntactically incorrect queries in the binary log, replacing some parameters with variable names rather than variable values. This could lead to incorrect results on replication slaves. (Bug #26842, Bug #12826)
- **Replication:** Connections from one `mysqld` server to another failed on Mac OS X, affecting replication and `FEDERATED` tables. (Bug #26664)

References: See also: Bug #29083.

- **Replication:** When using transactions and replication, shutting down the master in the middle of a transaction would cause all slaves to stop replicating. (Bug #22725)
- **Replication:** Using `CREATE TABLE LIKE ...` would raise an assertion when replicated to a slave. (Bug #18950)
- On the IBM i5 platform, the installation script in the `.savf` binaries unconditionally executed the `mysql_install_db` script. This problem was fixed in a repackaged distribution numbered 5.0.44b. (Bug #30084)
- Long path names for internal temporary tables could cause stack overflows. (Bug #29015)
- Using an `INTEGER` column from a table to `ROUND()` a number produced different results than using a constant with the same value as the `INTEGER` column. (Bug #28980)
- If a program binds a given number of parameters to a prepared statement handle and then somehow changes `stmt->param_count` to a different number, `mysql_stmt_execute()` could crash the client or server. (Bug #28934)
- `INSERT .. ON DUPLICATE KEY UPDATE` could under some circumstances silently update rows when it should not have. (Bug #28904)
- Queries that used `UUID()` were incorrectly permitted into the query cache. (This should not happen because `UUID()` is nondeterministic.) (Bug #28897)
- Using a `VIEW` created with a nonexisting `DEFINER` could lead to incorrect results under some circumstances. (Bug #28895)
- For `InnoDB` tables that use the `utf8` character set, incorrect results could occur for DML statements such as `DELETE` or `UPDATE` that use an index on character-based columns. (Bug #28878)

References: See also: Bug #29449, Bug #30485, Bug #31395. This issue is a regression of: Bug #13195.

- On Windows, `USE_TLS` was not defined for `mysqlclient.lib`. (Bug #28860)
- A subquery with `ORDER BY` and `LIMIT 1` could cause a server crash. (Bug #28811)
- Using `BETWEEN` with nonindexed date columns and short formats of the date string could return incorrect results. (Bug #28778)
- Selecting `GEOMETRY` columns in a `UNION` caused a server crash. (Bug #28763)
- When constructing the path to the original `.frm` file, `ALTER .. RENAME` was unnecessarily (and incorrectly) lowercasing the entire path when not on a case-insensitive file system, causing the statement to fail. (Bug #28754)
- Searches on indexed and nonindexed `ENUM` columns could return different results for empty strings. (Bug #28729)

- Executing `EXPLAIN EXTENDED` on a query using a derived table over a grouping subselect could lead to a server crash. This occurred only when materialization of the derived tables required creation of an auxiliary temporary table, an example being when a grouping operation was carried out with usage of a temporary table. (Bug #28728)
- The result of evaluation for a view's `CHECK OPTION` option over an updated record and records of merged tables was arbitrary and dependent on the order of records in the merged tables during the execution of the `SELECT` statement. (Bug #28716)
- The “manager thread” of the LinuxThreads implementation was unintentionally started before `mysqld` had dropped privileges (to run as an unprivileged user). This caused signaling between threads in `mysqld` to fail when the privileges were finally dropped. (Bug #28690)
- For debug builds, `ALTER TABLE` could trigger an assertion failure due to occurrence of a deadlock when committing changes. (Bug #28652)
- Killing from one connection a long-running `EXPLAIN QUERY` started from another connection caused `mysqld` to crash. (Bug #28598)
- Outer join queries with `ON` conditions over constant outer tables did not return `NULL`-complemented rows when conditions were evaluated to `FALSE`. (Bug #28571)
- An update on a multiple-table view with the `CHECK OPTION` clause and a subquery in the `WHERE` condition could cause an assertion failure. (Bug #28561)
- `PURGE MASTER LOGS BEFORE (subquery)` caused a server crash. Subqueries are forbidden in the `BEFORE` clause now. (Bug #28553)
- `mysqldump` calculated the required memory for a hex-blob string incorrectly causing a buffer overrun. This in turn caused `mysqldump` to crash silently and produce incomplete output. (Bug #28522)
- Passing a `DECIMAL` value as a parameter of a statement prepared with `PREPARE` resulted in an error. (Bug #28509)
- `mysql_affected_rows()` could return an incorrect result for `INSERT ... ON DUPLICATE KEY UPDATE` if the `CLIENT_FOUND_ROWS` flag was set. (Bug #28505)
- A query that grouped by the result of an expression returned a different result when the expression was assigned to a user variable. (Bug #28494)
- Subselects returning `LONG` values in MySQL versions later than 5.0.24a returned `LONGLONG` prior to this. The previous behavior was restored. (Bug #28492)

References: This issue is a regression of: Bug #19714.

- Forcing the use of an index on a `SELECT` query when the index had been disabled would raise an error without running the query. The query now executes, with a warning generated noting that the use of a disabled index has been ignored. (Bug #28476)
- The query `SELECT '2007-01-01' + INTERVAL column_name DAY FROM table_name` caused `mysqld` to fail. (Bug #28450)
- A server crash could happen under rare conditions such that a temporary table outgrew heap memory reserved for it and the remaining disk space was not big enough to store the table as a `MyISAM` table. (Bug #28449)
- `mysql_upgrade` failed if certain SQL modes were set. Now it sets the mode itself to avoid this problem. (Bug #28401)

- The test case for `mysqldump` failed with `bin-log` disabled. (Bug #28372)
- Attempting to `LOAD_FILE` from an empty floppy drive under Windows, caused the server to hang. For example, if you opened a connection to the server and then issued the command `SELECT LOAD_FILE('a:test');`, with no floppy in the drive, the server was inaccessible until the modal pop-up dialog box was dismissed. (Bug #28366)
- A buffer overflow could occur when using `DECIMAL` columns on Windows operating systems. (Bug #28361)
- `libmysql.dll` could not be dynamically loaded on Windows. (Bug #28358)
- Grouping queries with correlated subqueries in `WHERE` conditions could produce incorrect results. (Bug #28337)
- `mysqltest` used a too-large stack size on PowerPC/Debian Linux, causing thread-creation failure for tests that use many threads. (Bug #28333)
- `EXPLAIN` for a query on an empty table immediately after its creation could result in a server crash. (Bug #28272)
- The `IS_UPDATABLE` column in the `INFORMATION_SCHEMA.VIEWS` table was not always set correctly. (Bug #28266)
- Comparing a `DATETIME` column value with a user variable yielded incorrect results. (Bug #28261)
- For `CAST()` of a `NULL` value with type `DECIMAL`, the return value was incorrectly initialized, producing a runtime error for binaries built using Visual C++ 2005. (Bug #28250)
- Portability problems caused by use of `isinf()` were corrected. (Bug #28240)
- When dumping procedures, `mysqldump --compact` generated output that restored the session variable `sql_mode` without first capturing it. When dumping routines, `mysqldump --compact` neither set nor retrieved the value of `sql_mode`. (Bug #28223)
- Comparison of the string value of a date showed as unequal to `CURTIME()`. Similar behavior was exhibited for `DATETIME` values. (Bug #28208)
- The `Bytes_received` and `Bytes_sent` status variables could hold only 32-bit values (not 64-bit values) on some platforms. (Bug #28149)
- Storing a large number into a `FLOAT` or `DOUBLE` column with a fixed length could result in incorrect truncation of the number if the column's length was greater than 31. (Bug #28121)
- `DECIMAL` values beginning with nine 9 digits could be incorrectly rounded. (Bug #27984)
- The second execution of a prepared statement from a `UNION` query with `ORDER BY RAND()` caused the server to crash. This problem could also occur when invoking a stored procedure containing such a query. (Bug #27937)
- For attempts to open a nonexistent table, the server should report `ER_NO_SUCH_TABLE` but sometimes reported `ER_TABLE_NOT_LOCKED`. (Bug #27907)
- A stored program that uses a variable name containing multibyte characters could fail to execute. (Bug #27876)
- `ON` conditions from `JOIN` expressions were ignored when checking the `CHECK OPTION` clause while updating a multiple-table view that included such a clause. (Bug #27827)

- On some systems, `udf_example.c` returned an incorrect result length. Also on some systems, `mysql-test-run.pl` could not find the shared object built from `udf_example.c`. (Bug #27741)
- `HASH` indexes on `VARCHAR` columns with binary collations did not ignore trailing spaces from strings before comparisons. This could result in duplicate records being successfully inserted into a `MEMORY` table with unique key constraints. A consequence was that internal `MEMORY` tables used for `GROUP BY` calculation contained duplicate rows that resulted in duplicate-key errors when converting those temporary tables to `MyISAM`, and that error was incorrectly reported as a `table is full` error. (Bug #27643)
- An error occurred trying to connect to `mysqld-debug.exe`. (Bug #27597)
- Selecting `MIN()` on an indexed column that contained only `NULL` values caused `NULL` to be returned for other result columns. (Bug #27573)
- If a stored function or trigger was killed, it aborted but no error was thrown, permitting the calling statement to continue without noticing the problem. This could lead to incorrect results. (Bug #27563)
- When `ALTER TABLE` was used to add a new `DATE` column with no explicit default value, `'0000-00-00'` was used as the default even if the SQL mode included the `NO_ZERO_DATE` mode to prohibit that value. A similar problem occurred for `DATETIME` columns. (Bug #27507)
- Using a `TEXT` local variable in a stored routine in an expression such as `SET var = SUBSTRING(var, 3)` produced an incorrect result. (Bug #27415)
- The error message for error number `137` did not report which database/table combination reported the problem. (Bug #27173)
- A large filesort could result in a division by zero error and a server crash. (Bug #27119)
- Some test suite files were missing from some MySQL-test packages. (Bug #26609)
- Statements within triggers ignored the value of the `low_priority_updates` system variable. (Bug #26162)

References: See also: Bug #29963.

- Running `CHECK TABLE` concurrently with a `SELECT`, `INSERT` or other statement on Windows could corrupt a `MyISAM` table. (Bug #25712)
- On Windows, connection handlers did not properly decrement the server's thread count when exiting. (Bug #25621)
- Due to a race condition, executing `FLUSH PRIVILEGES` in one thread could cause brief table unavailability in other threads. (Bug #24988)
- When `mysqld` was run as a Windows service, shared memory objects were not created in the global namespace and could not be used by clients to connect. (Bug #24731)
- On some Linux distributions where `LinuxThreads` and `NPTL glibc` versions both are available, statically built binaries can crash because the linker defaults to `LinuxThreads` when linking statically, but calls to external libraries (such as `libnss`) are resolved to `NPTL` versions. This cannot be worked around in the code, so instead if a crash occurs on such a binary/OS combination, print an error message that provides advice about how to fix the problem. (Bug #24611)
- Implicit conversion of `9912101` to `DATE` did not match `CAST(9912101 AS DATE)`. (Bug #23093)

- Conversion errors could occur when constructing the condition for an `IN` predicate. The predicate was treated as if the affected column contains `NULL`, but if the `IN` predicate is inside `NOT`, incorrect results could be returned. (Bug #22855)
- Linux binaries were unable to dump core after executing a `setuid()` call. (Bug #21723)
- Stack overflow caused server crashes. (Bug #21476)
- `CURDATE()` is less than `NOW()`, either when comparing `CURDATE()` directly (`CURDATE() < NOW()` is true) or when casting `CURDATE()` to `DATE` (`CAST(CURDATE() AS DATE) < NOW()` is true). However, storing `CURDATE()` in a `DATE` column and comparing `col_name < NOW()` incorrectly yielded false. This is fixed by comparing a `DATE` column as `DATETIME` for comparisons to a `DATETIME` constant. (Bug #21103)
- For dates with 4-digit year parts less than 200, an incorrect implicit conversion to add a century was applied for date arithmetic performed with `DATE_ADD()`, `DATE_SUB()`, `+ INTERVAL`, and `- INTERVAL`. (For example, `DATE_ADD('0050-01-01 00:00:00', INTERVAL 0 SECOND)` became `'2050-01-01 00:00:00'`.) (Bug #18997)
- Granting access privileges to an individual table where the database or table name contained an underscore failed. (Bug #18660)
- The `-lmtmalloc` library was removed from the output of `mysql_config` on Solaris, as it caused problems when building `DBD:mysql` (and possibly other applications) on that platform that tried to use `dlopen()` to access the client library. (Bug #18322)
- The `check-cpu` script failed to detect AMD64 Turion processors correctly. (Bug #17707)
- Trying to shut down the server following a failed `LOAD DATA INFILE` caused `mysqld` to crash. (Bug #17233)
- Using up-arrow for command-line recall in `mysql` could cause a segmentation fault. (Bug #10218)
- The result for `CAST()` when casting a value to `UNSIGNED` was limited to the maximum signed `BIGINT` value (9223372036854775808), rather than the maximum unsigned value (18446744073709551615). (Bug #8663)

Changes in MySQL Enterprise 5.0.42 [MRU] (2007-05-23)

This is a *Monthly Rapid Update* release of the MySQL Enterprise Server 5.0.

This section documents all changes and bug fixes that have been applied since the last MySQL Enterprise Server release (5.0.40).

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- **Incompatible Change:** Prior to this release, when `DATE` values were compared with `DATETIME` values, the time portion of the `DATETIME` value was ignored, or the comparison could be performed as a string compare. Now a `DATE` value is coerced to the `DATETIME` type by adding the time portion as `00:00:00`. To mimic the old behavior, use the `CAST()` function as shown in this example: `SELECT date_col = CAST(NOW() AS DATE) FROM table;` (Bug #28929)
- **Incompatible Change:** `INSERT DELAYED` is now downgraded to a normal `INSERT` if the statement uses functions that access tables or triggers, or that is called from a function or a trigger.

This was done to resolve the following interrelated issues:

- The server could abort or deadlock for `INSERT DELAYED` statements for which another insert was performed implicitly (for example, using a stored function that inserted a row).
- A trigger using an `INSERT DELAYED` caused the error `INSERT DELAYED can't be used with table ... because it is locked with LOCK TABLES` although the target table was not actually locked.
- `INSERT DELAYED` into a table with a `BEFORE INSERT` or `AFTER INSERT` trigger gave an incorrect `NEW` pseudocolumn value and caused the server to deadlock or abort.

(Bug #21483)

References: See also: Bug #20497, Bug #21714.

- `mysqld_multi` now understands the `--no-defaults`, `--defaults-file`, and `--defaults-extra-file` options. The `--config-file` option is deprecated; if given, it is treated like `--defaults-extra-file`. (Bug #27390)

Bugs Fixed

- **Security Fix:** Use of a view could enable a user to gain update privileges for tables in other databases. (Bug #27878, CVE-2007-3782)
- **Security Fix:** The requirement of the `DROP` privilege for `RENAME TABLE` was not enforced. (Bug #27515, CVE-2007-2691)
- **Security Fix:** If a stored routine was declared using `SQL SECURITY INVOKER`, a user who invoked the routine could gain privileges. (Bug #27337, CVE-2007-2692)
- **MySQL Cluster:** The cluster waited 30 seconds instead of 30 milliseconds before reading table statistics. (Bug #28093)
- **MySQL Cluster:** `INSERT IGNORE` wrongly ignored `NULL` values in unique indexes. (Bug #27980)
- **MySQL Cluster:** The name of the month “March” was given incorrectly in the cluster error log. (Bug #27926)
- **MySQL Cluster:** It was not possible to add a unique index to an `NDB` table while in single user mode. (Bug #27710)
- **MySQL Cluster:** Repeated insertion of data generated by `mysqldump` into `NDB` tables could eventually lead to failure of the cluster. (Bug #27437)
- **MySQL Cluster:** `ndb_connectstring` did not appear in the output of `SHOW VARIABLES`. (Bug #26675)
- **Replication:** Aborting a statement on the master that applied to a nontransactional statement broke replication. The statement was written to the binary log but not completely executed on the master. Slaves receiving the statement executed it completely, resulting in loss of data synchrony. Now an error code is written to the error log so that the slaves stop without executing the aborted statement. (That is, replication stops, but synchrony to the point of the stop is preserved and you can investigate the problem.) (Bug #26551)
- **Replication:** Restoration of the default database after stored routine or trigger execution on a slave could cause replication to stop if the database no longer existed. (Bug #25082)

- **Cluster API:** For `BLOB` reads on operations with lock mode `LM_CommittedRead`, the lock mode was not upgraded to `LM_Read` before the state of the `BLOB` had already been calculated. The `NDB` API methods affected by this problem included the following:
 - `NdbOperation::readTuple()`
 - `NdbScanOperation::readTuples()`
 - `NdbIndexScanOperation::readTuples()`(Bug #27320)
- On the IBM i5 platform, the installation script in the `.saf` binaries unconditionally executed the `mysql_install_db` script. This problem was fixed in a repackaged distribution numbered 5.0.42b. (Bug #30084)
- A query with a `NOT IN` subquery predicate could cause a crash when the left operand of the predicate evaluated to `NULL`. (Bug #28375)
- For `InnoDB`, in some rare cases the optimizer preferred a more expensive `ref` access to a less expensive range access. (Bug #28189)
- A performance degradation was observed for outer join queries to which a not-exists optimization was applied. (Bug #28188)
- `SELECT * INTO OUTFILE ... FROM INFORMATION_SCHEMA.SCHEMATA` failed with an `Access denied` error, even for a user who had the `FILE` privilege. (Bug #28181)
- Comparisons of `DATE` or `DATETIME` values for the `IN()` function could yield incorrect results. (Bug #28133)
- The server could hang for `INSERT IGNORE ... ON DUPLICATE KEY UPDATE` if an update failed. (Bug #28000)
- `CAST()` to `DECIMAL` did not check for overflow. (Bug #27957)
- For `INSERT ... ON DUPLICATE KEY UPDATE` statements that affected many rows, updates could be applied to the wrong rows. (Bug #27954)
- Early `NULL`-filtering optimization did not work for `eq_ref` table access. (Bug #27939)
- Views ignored precision for `CAST()` operations. (Bug #27921)
- Nongrouped columns were permitted by `*` in `ONLY_FULL_GROUP_BY` SQL mode. (Bug #27874)
- Debug builds on Windows generated false alarms about uninitialized variables with some Visual Studio runtime libraries. (Bug #27811)
- Certain queries that used uncorrelated scalar subqueries caused `EXPLAIN` to crash. (Bug #27807)
- Changes to some system variables should invalidate statements in the query cache, but invalidation did not happen. (Bug #27792)
- Performing a `UNION` on two views that had `ORDER BY` clauses resulted in an `Unknown column` error. (Bug #27786)
- `mysql_install_db` is supposed to detect existing system tables and create only those that do not exist. Instead, it was exiting with an error if tables already existed. (Bug #27783)

- `mysqld` did not check the length of option values and could crash with a buffer overflow for long values. (Bug #27715)
- Comparisons using row constructors could fail for rows containing `NULL` values. (Bug #27704)
- `LOAD DATA` did not use `CURRENT_TIMESTAMP` as the default value for a `TIMESTAMP` column for which no value was provided. (Bug #27670)
- `mysqldump` could not connect using SSL. (Bug #27669)
- On Linux, the server could not create temporary tables if `lower_case_table_names` was set to 1 and the value of `tmpdir` was a directory name containing any uppercase letters. (Bug #27653)
- For InnoDB tables, a multiple-row `INSERT` of the form `INSERT INTO t (id...) VALUES (NULL...) ON DUPLICATE KEY UPDATE id=VALUES(id)`, where `id` is an `AUTO_INCREMENT` column, could cause `ERROR 1062 (23000): Duplicate entry...` errors or lost rows. (Bug #27650)
- The XML output representing an empty result was an empty string rather than an empty `<resultset/>` element. (Bug #27608)
- Comparison of a `DATE` with a `DATETIME` did not treat the `DATE` as having a time part of `00:00:00`. (Bug #27590)

References: See also: Bug #32198.

- The fix for Bug #17212 provided correct sort order for misordered output of certain queries, but caused significant overall query performance degradation. (Results were correct (good), but returned much more slowly (bad).) The fix also affected performance of queries for which results were correct. The performance degradation has been addressed. (Bug #27531)

References: This issue is a regression of: Bug #17212.

- The `CRC32()` function returns an unsigned integer, but the metadata was signed, which could cause certain queries to return incorrect results. (For example, queries that selected a `CRC32()` value and used that value in the `GROUP BY` clause.) (Bug #27530)
- An interaction between `SHOW TABLE STATUS` and other concurrent statements that modify the table could result in a divide-by-zero error and a server crash. (Bug #27516)
- A race condition between `DROP TABLE` and `SHOW TABLE STATUS` could cause the latter to display incorrect information. (Bug #27499)
- Nested aggregate functions could be improperly evaluated. (Bug #27363)
- A stored function invocation in the `WHERE` clause was treated as a constant. (Bug #27354)
- Failure to allocate memory associated with `transaction_prealloc_size` could cause a server crash. (Bug #27322)
- `mysqldump` crashed if it got no data from `SHOW CREATE PROCEDURE` (for example, when trying to dump a routine defined by a different user and for which the current user had no privileges). Now it prints a comment to indicate the problem. It also returns an error, or continues if the `--force` option is given. (Bug #27293)
- `mysqlbinlog` produced different output with the `-R` option than without it. (Bug #27171)
- Flow control optimization in stored routines could cause exception handlers to never return or execute incorrect logic. (Bug #26977)

- `mysqldump` would not dump a view for which the `DEFINER` no longer exists. (Bug #26817)
- Creating a temporary table with `InnoDB` when using the one-file-per-table setting, and when the host file system for temporary tables was `tmpfs`, would cause an assertion within `mysqld`. This was due to the use of `O_DIRECT` when opening the temporary table file. (Bug #26662)
- `mysql_upgrade` did not detect failure of external commands that it runs. (Bug #26639)
- Index hints (`USE INDEX`, `IGNORE INDEX`, `FORCE INDEX`) cannot be used with `FULLTEXT` indexes, but were not being ignored. (Bug #25951)
- If `CREATE TABLE t1 LIKE t2` failed due to a full disk, an empty `t2.frm` file could be created but not removed. This file then caused subsequent attempts to create a table named `t2` to fail. This is easily corrected at the file system level by removing the `t2.frm` file manually, but now the server removes the file if the create operation does not complete successfully. (Bug #25761)
- `mysql_upgrade` did not pass a password to `mysqlcheck` if one was given. (Bug #25452)
- On Windows, `mysql_upgrade` was sensitive to lettercase of the names of some required components. (Bug #25405)
- For storage engines that permit the current auto-increment value to be set, using `ALTER TABLE ... ENGINE` to convert a table from one such storage engine to another caused loss of the current value. (For storage engines that do not support setting the value, it cannot be retained anyway when changing the storage engine.) (Bug #25262)
- Several math functions produced incorrect results for large unsigned values. `ROUND()` produced incorrect results or a crash for a large number-of-decimals argument. (Bug #24912)
- The result set of a query that used `WITH ROLLUP` and `DISTINCT` could lack some rollup rows (rows with `NULL` values for grouping attributes) if the `GROUP BY` list contained constant expressions. (Bug #24856)
- For queries that used `ORDER BY` with `InnoDB` tables, if the optimizer chose an index for accessing the table but found a covering index that enabled the `ORDER BY` to be skipped, no results were returned. (Bug #24778)
- Concurrent execution of `CREATE TABLE ... SELECT` and other statements involving the target table suffered from various race conditions, some of which might have led to deadlocks. (Bug #24738)
- An attempt to execute `CREATE TABLE ... SELECT` when a temporary table with the same name already existed led to the insertion of data into the temporary table and creation of an empty nontemporary table. (Bug #24508)
- The `MERGE` storage engine could return incorrect results when several index values that compare equality were present in an index (for example, `'gross'` and `'gross '`, which are considered equal but have different lengths). (Bug #24342)
- Some upgrade problems are detected and better error messages suggesting that `mysql_upgrade` be run are produced. (Bug #24248)
- Some views could not be created even when the user had the requisite privileges. (Bug #24040)
- Using `CAST()` to convert `DATETIME` values to numeric values did not work. (Bug #23656)
- The `AUTO_INCREMENT` value would not be correctly reported for `InnoDB` tables when using `SHOW CREATE TABLE` statement or `mysqldump` command. (Bug #23313)

- `SELECT COUNT(*)` from a table containing a `DATETIME NOT NULL` column could produce spurious warnings with the `NO_ZERO_DATE` SQL mode enabled. (Bug #22824)
- Using `SET GLOBAL` to change the `lc_time_names` system variable had no effect on new connections. (Bug #22648)
- A multiple-table `UPDATE` could return an incorrect rows-matched value if, during insertion of rows into a temporary table, the table had to be converted from a `MEMORY` table to a `MyISAM` table. (Bug #22364)
- `yaSSL` crashed on pre-Pentium Intel CPUs. (Bug #21765)
- A slave that used `--master-ssl-cipher` could not connect to the master. (Bug #21611)
- Quoted labels in stored routines were mishandled, rendering the routines unusable. (Bug #21513)
- `CREATE TABLE IF NOT EXISTS ... SELECT` caused a server crash if the target table already existed and had a `BEFORE INSERT` trigger. (Bug #20903)
- Deadlock occurred for attempts to execute `CREATE TABLE IF NOT EXISTS ... SELECT` when `LOCK TABLES` had been used to acquire a read lock on the target table. (Bug #20662, Bug #15522)
- Changing a `utf8` column in an `InnoDB` table to a shorter length did not shorten the data values. (Bug #20095)
- The omission of leading zeros in dates could lead to erroneous results when these were compared with the output of certain date and time functions. (Bug #16377)
- `INSERT...ON DUPLICATE KEY UPDATE` could cause `Error 1032: Can't find record in ...` for inserts into an `InnoDB` table unique index using key column prefixes with an underlying `utf8` string column. (Bug #13191)
- Having the `EXECUTE` privilege for a routine in a database should make it possible to `USE` that database, but the server returned an error instead. This has been corrected. As a result of the change, `SHOW TABLES` for a database in which you have only the `EXECUTE` privilege returns an empty set rather than an error. (Bug #9504)

Changes in MySQL Community Server 5.0.41 (2007-05-01)

This is a bugfix release for the current MySQL Community Server production release family. It replaces MySQL 5.0.37.

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- If a set function `S` with an outer reference `S(outer_ref)` cannot be aggregated in the outer query against which the outer reference has been resolved, MySQL interprets `S(outer_ref)` the same way that it would interpret `S(const)`. However, standard SQL requires throwing an error in this situation. An error now is thrown for such queries if the `ANSI` SQL mode is enabled. (Bug #27348)
- Prefix lengths for columns in `SPATIAL` indexes are no longer displayed in `SHOW CREATE TABLE` output. `mysqldump` uses that statement, so if a table with `SPATIAL` indexes containing prefixed columns is dumped and reloaded, the index is created with no prefixes. (The full column width of each column is indexed.) (Bug #26794)
- The output of `mysql --xml` and `mysqldump --xml` now includes a valid XML namespace. (Bug #25946)

- If you use SSL for a client connection, you can tell the client not to authenticate the server certificate by specifying neither `--ssl-ca` nor `--ssl-capath`. The server still verifies the client according to any applicable requirements established using `GRANT` statements for the client, and it still uses any `--ssl-ca/--ssl-capath` values that were passed to server at startup time. (Bug #25309)
- The server now includes a timestamp in error messages that are logged as a result of unhandled signals (such as `mysqld got signal 11` messages). (Bug #24878)
- The syntax for index hints has been extended to enable explicit specification that the hint applies only to join processing. See [Index Hints](#).

This is a new fix for this issue, and replaces the fix made in MySQL 5.0.25 and reverted in 5.0.26. (Bug #21174)

- Added the `--secure-file-priv` option for `mysqld`, which limits the effect of the `LOAD_FILE()` function and the `LOAD DATA` and `SELECT ... INTO OUTFILE` statements to work only with files in a given directory. (Bug #18628)
- Binary distributions for some platforms did not include shared libraries; now shared libraries are shipped for all platforms except AIX 5.2 64-bit. *Exception:* The library for the `libmysqld` embedded server is not shared except on Windows. (Bug #16520, Bug #26767, Bug #13450)
- Added the read-only `hostname` system variable, which the server sets at startup to the server host name.
- The `mysql_create_system_tables` script was removed because `mysql_install_db` no longer uses it.
- To satisfy different user requirements, we provide several servers. `mysqld` is an optimized server that is a smaller, faster binary. Each package now also includes `mysqld-debug`, which is compiled with debugging support but is otherwise configured identically to the nondebug server.

Bugs Fixed

- **Incompatible Change:** `INSERT DELAYED` statements are not supported for `MERGE` tables, but the `MERGE` storage engine was not rejecting such statements, resulting in table corruption. Applications previously using `INSERT DELAYED` into `MERGE` table will break when upgrading to versions with this fix. To avoid the problem, remove `DELAYED` from such statements. (Bug #26464)
- **MySQL Cluster:** `NDB` tables having `MEDIUMINT AUTO_INCREMENT` columns were not restored correctly by `ndb_restore`, causing spurious duplicate key errors. This issue did not affect `TINYINT`, `INT`, or `BIGINT` columns with `AUTO_INCREMENT`. (Bug #27775)
- **MySQL Cluster:** `NDB` tables with indexes whose names contained space characters were not restored correctly by `ndb_restore` (the index names were truncated). (Bug #27758)
- **MySQL Cluster:** Under certain rare circumstances performing a `DROP TABLE` or `TRUNCATE TABLE` on an `NDB` table could cause a node failure or forced cluster shutdown. (Bug #27581)
- **MySQL Cluster:** Memory usage of a `mysqld` process grew even while idle. (Bug #27560)
- **MySQL Cluster:** It was not possible to set `LockPagesInMainMemory` equal to 0. (Bug #27291)
- **MySQL Cluster:** A race condition could sometimes occur if the node acting as master failed while node IDs were still being allocated during startup. (Bug #27286)
- **MySQL Cluster:** When a data node was taking over as the master node, a race condition could sometimes occur as the node was assuming responsibility for handling of global checkpoints. (Bug #27283)

- **MySQL Cluster:** Error messages displayed when running in single user mode were inconsistent. (Bug #27021)
- **MySQL Cluster:** The failure of a data node while restarting could cause other data nodes to hang or crash. (Bug #27003)
- **MySQL Cluster:** On Solaris, the value of an NDB table column declared as `BIT(33)` was always displayed as `0`. (Bug #26986)
- **MySQL Cluster:** `mysqld` processes would sometimes crash under high load. (Bug #26825)
- **MySQL Cluster:** The output from `ndb_restore --print_data` was incorrect for a backup made of a database containing tables with `TINYINT` or `SMALLINT` columns. (Bug #26740)
- **MySQL Cluster:** An inadvertent use of unaligned data caused `ndb_restore` to fail on some 64-bit platforms, including Sparc and Itanium-2. (Bug #26739)
- **MySQL Cluster:** An invalid pointer was returned following a `FSCLOSECONF` signal when accessing the REDO logs during a node restart or system restart. (Bug #26515)
- **MySQL Cluster:** The failure of a data node when restarting it with `--initial` could lead to failures of subsequent data node restarts. (Bug #26481)
- **MySQL Cluster:** Takeover for local checkpointing due to multiple failures of master nodes was sometimes incorrectly handled. (Bug #26457)
- **MySQL Cluster:** The `LockPagesInMainMemory` parameter was not read until after distributed communication had already started between cluster nodes. When the value of this parameter was `1`, this could sometimes result in data node failure due to missed heartbeats. (Bug #26454)
- **MySQL Cluster:** Under some circumstances, following the restart of a management node, all data nodes would connect to it normally, but some of them subsequently failed to log any events to the management node. (Bug #26293)
- **MySQL Cluster:** In some cases, `AFTER UPDATE` and `AFTER DELETE` triggers on NDB tables that referenced subject table did not see the results of operation which caused invocation of the trigger, but rather saw the row as it was prior to the update or delete operation.

This was most noticeable when an update operation used a subquery to obtain the rows to be updated. An example would be `UPDATE tbl1 SET col2 = val1 WHERE tbl1.col1 IN (SELECT col3 FROM tbl2 WHERE c4 = val2)` where there was an `AFTER UPDATE` trigger on table `tbl1`. In such cases, the trigger failed to execute.

The problem occurred because the actual update or delete operations were deferred to be able to perform them later as one batch. The fix for this bug solves the problem by disabling this optimization for a given update or delete if the table has an `AFTER` trigger defined for this operation. (Bug #26242)

- **MySQL Cluster:** Condition pushdown did not work with prepared statements. (Bug #26225)
- **MySQL Cluster:** Joins on multiple tables containing `BLOB` columns could cause data nodes run out of memory, and to crash with the error `NdbObjectIdMap::expand unable to expand`. (Bug #26176)
- **MySQL Cluster:** After entering single user mode it was not possible to alter non-NDB tables on any SQL nodes other than the one having sole access to the cluster. (Bug #25275)
- **MySQL Cluster:** The management client command `node_id STATUS` displayed the message `Node node_id: not connected` when `node_id` was not the node ID of a data node.

**Note**

The `ALL STATUS` command in the cluster management client still displays status information for data nodes only. This is by design. See [Commands in the MySQL Cluster Management Client](#), for more information.

(Bug #21715)

- **MySQL Cluster:** The message `Error 0 in readAutoIncrementValue(): no Error` was written to the error log whenever `SHOW TABLE STATUS` was performed on a Cluster table that did not have an `AUTO_INCREMENT` column. (Bug #21033)
- **MySQL Cluster:** Some values of `MaxNoOfTables` caused the error `Job buffer congestion` to occur. (Bug #19378)
- **Replication:** Out-of-memory errors were not reported. Now they are written to the error log. (Bug #26844)
- **Replication:** Improved out-of-memory detection when sending logs from a master server to slaves, and log a message when allocation fails. (Bug #26837)
- **Replication:** A multiple-row delayed insert with an auto-increment column could cause duplicate entries to be created on the slave in a replication environment. (Bug #26116, Bug #25507)
- **Replication:** When `RAND()` was called multiple times inside a stored procedure, the server did not write the correct random seed values to the binary log, resulting in incorrect replication. (Bug #25543)
- **Replication:** `GRANT` statements were not replicated if the server was started with the `--replicate-ignore-table` or `--replicate-wild-ignore-table` option. (Bug #25482)
- **Replication:** Duplicating the usage of a user variable in a stored procedure or trigger would not be replicated correctly to the slave. (Bug #25167)
- **Replication:** `DROP TRIGGER` statements would not be filtered on the slave when using the `replication-wild-do-table` option. (Bug #24478)
- **Replication:** For `INSERT ... ON DUPLICATE KEY UPDATE` statements where some `AUTO_INCREMENT` values were generated automatically for inserts and some rows were updated, one auto-generated value was lost per updated row, leading to faster exhaustion of the range of the `AUTO_INCREMENT` column.

Because the original problem can affect replication (different values on master and slave), it is recommended that the master and its slaves be upgraded to the current version. (Bug #24432)
- **Replication:** Replication between master and slave would infinitely retry binary log transmission where the `max_allowed_packet` on the master was larger than that on the slave if the size of the transfer was between these two values. (Bug #23775)
- **Replication:** Loading data using `LOAD DATA INFILE` may not replicate correctly (due to character set incompatibilities) if the `character_set_database` variable is set before the data is loaded. (Bug #15126)
- **Replication:** User defined variables used within stored procedures and triggers are not replicated correctly when operating in statement-based replication mode. (Bug #14914, Bug #20141)
- **Cluster Replication:** Some queries that updated multiple tables were not backed up correctly. (Bug #27748)

- **Cluster API:** Using `NdbBlob::writeData()` to write data in the middle of an existing blob value (that is, updating the value) could overwrite some data past the end of the data to be changed. (Bug #27018)
- Some equi-joins containing a `WHERE` clause that included a `NOT IN` subquery caused a server crash. (Bug #27870)
- `SELECT DISTINCT` could return incorrect results if the select list contained duplicated columns. (Bug #27659)
- With `NO_AUTO_VALUE_ON_ZERO` SQL mode enabled, `LOAD DATA` operations could assign incorrect `AUTO_INCREMENT` values. (Bug #27586)
- Incorrect results could be returned for some queries that contained a select list expression with `IN` or `BETWEEN` together with an `ORDER BY` or `GROUP BY` on the same expression using `NOT IN` or `NOT BETWEEN`. (Bug #27532)
- Evaluation of an `IN()` predicate containing a decimal-valued argument caused a server crash. (Bug #27513, Bug #27362, CVE-2007-2583)
- Profiling overhead was incurred even with profiling disabled. (Bug #27501)
- In out-of-memory conditions, the server might crash or otherwise not report an error to the Windows event log. (Bug #27490)
- Passing nested row expressions with different structures to an `IN` predicate caused a server crash. (Bug #27484)
- The `decimal.h` header file was incorrectly omitted from binary distributions. (Bug #27456)
- With `innodb_file_per_table` enabled, attempting to rename an `InnoDB` table to a nonexistent database caused the server to exit. (Bug #27381)
- A subquery could get incorrect values for references to outer query columns when it contained aggregate functions that were aggregated in outer context. (Bug #27321)
- In a view, a column that was defined using a `GEOMETRY` function was treated as having the `LONGBLOB` data type rather than the `GEOMETRY` type. (Bug #27300)
- Queries containing subqueries with `COUNT(*)` aggregated in an outer context returned incorrect results. This happened only if the subquery did not contain any references to outer columns. (Bug #27257)
- `SELECT ... INTO OUTFILE` with a long `FIELDS ENCLOSED BY` value could crash the server. (Bug #27231)
- Use of an aggregate function from an outer context as an argument to `GROUP_CONCAT()` caused a server crash. (Bug #27229)
- String truncation upon insertion into an integer or year column did not generate a warning (or an error in strict mode). (Bug #27176, Bug #26359)
- Storing `NULL` values in spatial fields caused excessive memory allocation and crashes on some systems. (Bug #27164)
- Row equalities in `WHERE` clauses could cause memory corruption. (Bug #27154)
- `GROUP BY` on a `ucs2` column caused a server crash when there was at least one empty string in the column. (Bug #27079)
- Duplicate members in `SET` or `ENUM` definitions were not detected. Now they result in a warning; if strict SQL mode is enabled, an error occurs instead. (Bug #27069)

- For `INSERT ... ON DUPLICATE KEY UPDATE` statements on tables containing `AUTO_INCREMENT` columns, `LAST_INSERT_ID()` was reset to 0 if no rows were successfully inserted or changed. “Not changed” includes the case where a row was updated to its current values, but in that case, `LAST_INSERT_ID()` should not be reset to 0. Now `LAST_INSERT_ID()` is reset to 0 only if no rows were successfully inserted or touched, whether or not touched rows were changed. (Bug #27033)

References: See also: Bug #27210, Bug #27006. This issue is a regression of: Bug #19978.

- `mysql_install_db` could terminate with an error after failing to determine that a system table already existed. (Bug #27022)
- `AFTER UPDATE` triggers were not activated by the update part of `INSERT ... ON DUPLICATE KEY UPDATE` statements. (Bug #27006)

References: See also: Bug #27033, Bug #27210. This issue is a regression of: Bug #19978.

- In a `MEMORY` table, using a `BTREE` index to scan for updatable rows could lead to an infinite loop. (Bug #26996)
- Invalid optimization of pushdown conditions for queries where an outer join was guaranteed to read only one row from the outer table led to results with too few rows. (Bug #26963)
- Windows binaries contained no debug symbol file. Now `.map` and `.pdb` files are included in 32-bit builds for `mysqld-nt.exe`, `mysqld-debug.exe`, and `mysqlmanager.exe`. (Bug #26893)
- For `MERGE` tables defined on underlying tables that contained a short `VARCHAR` column (shorter than four characters), using `ALTER TABLE` on at least one but not all of the underlying tables caused the table definitions to be considered different from that of the `MERGE` table, even if the `ALTER TABLE` did not change the definition. (Bug #26881)
- For `InnoDB` tables having a clustered index that began with a `CHAR` or `VARCHAR` column, deleting a record and then inserting another before the deleted record was purged could result in table corruption. (Bug #26835)
- Use of a subquery containing `GROUP BY` and `WITH ROLLUP` caused a server crash. (Bug #26830)
- Duplicates were not properly identified among (potentially) long strings used as arguments for `GROUP_CONCAT(DISTINCT)`. (Bug #26815)
- `ALTER VIEW` requires the `CREATE VIEW` and `DROP` privileges for the view. However, if the view was created by another user, the server erroneously required the `SUPER` privilege. (Bug #26813)
- Added support for `--debugger=dbx` for `mysql-test-run.pl` and added support for `--debugger=devenv`, `--debugger=DevEnv`, and `--debugger=/path/to/devenv`. (Bug #26792)
- A result set column formed by concatenation of string literals was incomplete when the column was produced by a subquery in the `FROM` clause. (Bug #26738)
- SSL connections failed on Windows. (Bug #26678)
- When using the result of `SEC_TO_TIME()` for time value greater than 24 hours in an `ORDER BY` clause, either directly or through a column alias, the rows were sorted incorrectly as strings. (Bug #26672)
- Use of a subquery containing a `UNION` with an invalid `ORDER BY` clause caused a server crash. (Bug #26661)
- The range optimizer could cause the server to run out of memory. (Bug #26625)

- The range optimizer could consume a combinatorial amount of memory for certain classes of `WHERE` clauses. (Bug #26624)
- In some error messages, inconsistent format specifiers were used for the translations in different languages. `comp_err` (the error message compiler) now checks for mismatches. (Bug #26571)
- Views that used a scalar correlated subquery returned incorrect results. (Bug #26560)
- `UNHEX() IS NULL` comparisons failed when `UNHEX()` returned `NULL`. (Bug #26537)
- On 64-bit Windows, large timestamp values could be handled incorrectly. (Bug #26536)
- `mysqldump` could crash or exhibit incorrect behavior when some options were given very long values, such as `--fields-terminated-by="some very long string"`. The code has been cleaned up to remove a number of fixed-sized buffers and to be more careful about error conditions in memory allocation. (Bug #26346)
- If the server was started with `--skip-grant-tables`, selecting from `INFORMATION_SCHEMA` tables caused a server crash. (Bug #26285)
- For some values of the position argument, the `INSERT()` function could insert a NUL byte into the result. (Bug #26281)
- For an `INSERT` statement that should fail due to a column with no default value not being assigned a value, the statement succeeded with no error if the column was assigned a value in an `ON DUPLICATE KEY UPDATE` clause, even if that clause was not used. (Bug #26261)
- `INSERT DELAYED` statements inserted incorrect values into `BIT` columns. (Bug #26238)
- The temporary file-creation code was cleaned up on Windows to improve server stability. (Bug #26233)
- For `MyISAM` tables, `COUNT(*)` could return an incorrect value if the `WHERE` clause compared an indexed `TEXT` column to the empty string (`' '`). This happened if the column contained empty strings and also strings starting with control characters such as tab or newline. (Bug #26231)
- For `INSERT INTO ... SELECT` where index searches used column prefixes, insert errors could occur when key value type conversion was done. (Bug #26207)
- For `DELETE FROM tbl_name ORDER BY col_name` (with no `WHERE` or `LIMIT` clause), the server did not check whether `col_name` was a valid column in the table. (Bug #26186)
- `REPAIR TABLE ... USE_FRM` with an `ARCHIVE` table deleted all records from the table. (Bug #26138)
- `BENCHMARK()` did not work correctly for expressions that produced a `DECIMAL` result. (Bug #26093)
- `LOAD DATA INFILE` sent an okay to the client before writing the binary log and committing the changes to the table had finished, thus violating ACID requirements. (Bug #26050)
- `X() IS NULL` and `Y() IS NULL` comparisons failed when `X()` and `Y()` returned `NULL`. (Bug #26038)
- `mysqldump` crashed for `MERGE` tables if the `--complete-insert (-c)` option was given. (Bug #25993)
- Indexes on `TEXT` columns were ignored when `ref` accesses were evaluated. (Bug #25971)
- If a thread previously serviced a connection that was killed, excessive memory and CPU use by the thread occurred if it later serviced a connection that had to wait for a table lock. (Bug #25966)
- Setting a column to `NOT NULL` with an `ON DELETE SET NULL` clause foreign key crashes the server. (Bug #25927)

- `VIEW` restrictions were applied to `SELECT` statements after a `CREATE VIEW` statement failed, as though the `CREATE` had succeeded. (Bug #25897)
- Several deficiencies in resolution of column names for `INSERT ... SELECT` statements were corrected. (Bug #25831)
- Inserting `utf8` data into a `TEXT` column that used a single-byte character set could result in spurious warnings about truncated data. (Bug #25815)
- On Windows, debug builds of `mysqld` could fail with heap assertions. (Bug #25765)
- In certain situations, `MATCH ... AGAINST` returned false hits for `NULL` values produced by `LEFT JOIN` when no full-text index was available. (Bug #25729)
- In certain cases it could happen that deleting a row corrupted an `RTREE` index. This affected indexes on spatial columns. (Bug #25673)
- `OPTIMIZE TABLE` might fail on Windows when it attempts to rename a temporary file to the original name if the original file had been opened, resulting in loss of the `.MYD` file. (Bug #25521)
- For `SHOW ENGINE INNODB STATUS`, the `LATEST DEADLOCK INFORMATION` was not always cleared properly. (Bug #25494)
- `mysql_stmt_fetch()` did an invalid memory deallocation when used with the embedded server. (Bug #25492)
- Expressions involving `SUM()`, when used in an `ORDER BY` clause, could lead to out-of-order results. (Bug #25376)
- Use of a `GROUP BY` clause that referred to a stored function result together with `WITH ROLLUP` caused incorrect results. (Bug #25373)
- A stored procedure that made use of cursors failed when the procedure was invoked from a stored function. (Bug #25345)
- Difficult repair or optimization operations could cause an assertion failure, resulting in a server crash. (Bug #25289)
- On Windows, the server exhibited a file-handle leak after reaching the limit on the number of open file descriptors. (Bug #25222)
- The `REPEAT()` function did not permit a column name as the `count` parameter. (Bug #25197)
- A reference to a nonexistent column in the `ORDER BY` clause of an `UPDATE ... ORDER BY` statement could cause a server crash. (Bug #25126)
- A view on a join is insertable for `INSERT` statements that store values into only one table of the join. However, inserts were being rejected if the inserted-into table was used in a self-join because MySQL incorrectly was considering the insert to modify multiple tables of the view. (Bug #25122)
- MySQL would not compile when configured using `--without-query-cache`. (Bug #25075)
- Duplicate entries were not assessed correctly in a `MEMORY` table with a `BTREE` primary key on a `utf8 ENUM` column. (Bug #24985)
- Selecting the result of `AVG()` within a `UNION` could produce incorrect values. (Bug #24791)
- `MBROverlaps()` returned incorrect values in some cases. (Bug #24563)
- Increasing the width of a `DECIMAL` column could cause column values to be changed. (Bug #24558)

- `IF(expr, unsigned_expr, unsigned_expr)` was evaluated to a signed result, not unsigned. This has been corrected. The fix also affects constructs of the form `IS [NOT] {TRUE|FALSE}`, which were transformed internally into `IF()` expressions that evaluated to a signed result.

For existing views that were defined using `IS [NOT] {TRUE|FALSE}` constructs, there is a related implication. The definitions of such views were stored using the `IF()` expression, not the original construct. This is manifest in that `SHOW CREATE VIEW` shows the transformed `IF()` expression, not the original one. Existing views will evaluate correctly after the fix, but if you want `SHOW CREATE VIEW` to display the original construct, you must drop the view and re-create it using its original definition. New views will retain the construct in their definition. (Bug #24532)

- A problem in handling of aggregate functions in subqueries caused predicates containing aggregate functions to be ignored during query execution. (Bug #24484)
- The test for the `MYSQL_OPT_SSL_VERIFY_SERVER_CERT` option for `mysql_options()` was performed incorrectly. Also changed as a result of this bug fix: The `arg` option for the `mysql_options()` C API function was changed from `char *` to `void *`. (Bug #24121)
- A user-defined variable could be assigned an incorrect value if a temporary table was employed in obtaining the result of the query used to determine its value. (Bug #24010)
- Queries that used a temporary table for the outer query when evaluating a correlated subquery could return incorrect results. (Bug #23800)
- On Windows, debug builds of `mysqlbinlog` could fail with a memory error. (Bug #23736)
- When using certain server SQL modes, the `mysql.proc` table was not created by `mysql_install_db`. (Bug #23669)
- The values displayed for the `Innodb_row_lock_time`, `Innodb_row_lock_time_avg`, and `Innodb_row_lock_time_max` status variables were incorrect. (Bug #23666)
- `DOUBLE` values such as `20070202191048.000000` were being treated as illegal arguments by `WEEK()`. (Bug #23616)
- The server could crash if two or more threads initiated query cache resize operation at moments very close in time. (Bug #23527)
- `SHOW CREATE VIEW` qualified references to stored functions in the view definition with the function's database name, even when the database was the default database. This affected `mysqldump` (which uses `SHOW CREATE VIEW` to dump views) because the resulting dump file could not be used to reload the database into a different database. `SHOW CREATE VIEW` now suppresses the database name for references to stored functions in the default database. (Bug #23491)
- An `INTO OUTFILE` clause is permitted only for the final `SELECT` of a `UNION`, but this restriction was not being enforced correctly. (Bug #23345)
- `NOW()` returned the wrong value in statements executed at server startup with the `--init-file` option. (Bug #23240)
- With the `NO_AUTO_VALUE_ON_ZERO` SQL mode enabled, `LAST_INSERT_ID()` could return 0 after `INSERT ... ON DUPLICATE KEY UPDATE`. Additionally, the next rows inserted (by the same `INSERT`, or the following `INSERT` with or without `ON DUPLICATE KEY UPDATE`), would insert 0 for the auto-generated value if the value for the `AUTO_INCREMENT` column was `NULL` or missing. (Bug #23233)
- `SOUNDEX()` returned an invalid string for international characters in multibyte character sets. (Bug #22638)

- When nesting stored procedures within a trigger on a table, a false dependency error was thrown when one of the nested procedures contained a `DROP TABLE` statement. (Bug #22580)
- Instance Manager did not remove the angel PID file on a clean shutdown. (Bug #22511)
- `EXPLAIN EXTENDED` did not show `WHERE` conditions that were optimized away. (Bug #22331)
- `COUNT(decimal_expr)` sometimes generated a spurious truncation warning. (Bug #21976)
- `IN ((subquery)), IN (((subquery)))`, and so forth, are equivalent to `IN (subquery)`, which is always interpreted as a table subquery (so that it is permitted to return more than one row). MySQL was treating the “over-parenthesized” subquery as a single-row subquery and rejecting it if it returned more than one row. This bug primarily affected automatically generated code (such as queries generated by Hibernate), because humans rarely write the over-parenthesized forms. (Bug #21904)
- An `INSERT` trigger invoking a stored routine that inserted into a table other than the one on which the trigger was defined failed with a `Table '...' doesn't exist` referring to the second table when attempting to delete records from the first table. (Bug #21825)
- `InnoDB`: The first read statement, if served from the query cache, was not consistent with the `READ COMMITTED` isolation level. (Bug #21409)
- `CURDATE()` is less than `NOW()`, either when comparing `CURDATE()` directly (`CURDATE() < NOW()` is true) or when casting `CURDATE()` to `DATE` (`CAST(CURDATE() AS DATE) < NOW()` is true). However, storing `CURDATE()` in a `DATE` column and comparing `col_name < NOW()` incorrectly yielded false. This is fixed by comparing a `DATE` column as `DATETIME` for comparisons to a `DATETIME` constant. (Bug #21103)
- When a stored routine attempted to execute a statement accessing a nonexistent table, the error was not caught by the routine's exception handler. (Bug #20713, Bug #8407)
- For a stored procedure containing a `SELECT` statement that used a complicated join with an `ON` expression, the expression could be ignored during re-execution of the procedure, yielding an incorrect result. (Bug #20492)
- The conditions checked by the optimizer to permit use of indexes in `IN` predicate calculations were unnecessarily tight and were relaxed. (Bug #20420)
- When a `TIME_FORMAT()` expression was used as a column in a `GROUP BY` clause, the expression result was truncated. (Bug #20293)
- The creation of MySQL system tables was not checked for by `mysql-test-run.pl`. (Bug #20166)
- For index reads, the `BLACKHOLE` engine did not return end-of-file (which it must because `BLACKHOLE` tables contain no rows), causing some queries to crash. (Bug #19717)
- In some cases, the optimizer preferred a range or full index scan access method over lookup access methods when the latter were much cheaper. (Bug #19372)
- For `expr IN(value_list)`, the result could be incorrect if `BIGINT UNSIGNED` values were used for `expr` or in the value list. (Bug #19342)
- When attempting to call a stored procedure creating a table from a trigger on a table `tbl` in a database `db`, the trigger failed with `ERROR 1146 (42S02): Table 'db.tbl' doesn't exist`. However, the actual reason that such a trigger fails is due to the fact that `CREATE TABLE` causes an implicit `COMMIT`, and so a trigger cannot invoke a stored routine containing this statement. A trigger which does so now fails with `ERROR 1422 (HY000): Explicit or implicit commit is not permitted`

`in stored function or trigger`, which makes clear the reason for the trigger's failure. (Bug #18914)

- The update columns for `INSERT ... SELECT ... ON DUPLICATE KEY UPDATE` could be assigned incorrect values if a temporary table was used to evaluate the `SELECT`. (Bug #16630)
- Conversion of `DATETIME` values in numeric contexts sometimes did not produce a double (`YYYYMMDDHHMMSS.uuuuuu`) value. (Bug #16546)
- For `SUBSTRING()` evaluation using a temporary table, when `SUBSTRING()` was used on a `LONGTEXT` column, the `max_length` metadata value of the result was incorrectly calculated and set to 0. Consequently, an empty string was returned instead of the correct result. (Bug #15757)
- Local variables in stored routines or triggers, when declared as the `BIT` type, were interpreted as strings. (Bug #12976)
- `CONNECTION` is no longer treated as a reserved word. (Bug #12204)

Changes in MySQL Enterprise 5.0.40 [MRU] (2007-04-17)

This is a *Monthly Rapid Update* release of the MySQL Enterprise Server 5.0.

This section documents all changes and bug fixes that have been applied since the last MySQL Enterprise Server release (5.0.38).

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- **MySQL Cluster:** The behavior of the `ndb_restore` utility has been changed as follows:
 - It is now possible to restore selected databases or tables using `ndb_restore`.
 - Several options have been added for use with `ndb_restore --print_data` to facilitate the creation of structured data dump files. These options can be used to make dumps made using `ndb_restore` more like those produced by `mysqldump`.

For details of these changes, see [ndb_restore — Restore a MySQL Cluster Backup](#). (Bug #26899, Bug #26900)

- If a set function `S` with an outer reference `S(outer_ref)` cannot be aggregated in the outer query against which the outer reference has been resolved, MySQL interprets `S(outer_ref)` the same way that it would interpret `S(const)`. However, standard SQL requires throwing an error in this situation. An error now is thrown for such queries if the `ANSI SQL` mode is enabled. (Bug #27348)
- Added the `--service-startup-timeout` option for `mysql.server` to specify how long to wait for the server to start. If the server does not start within the timeout period, `mysql.server` exits with an error. (Bug #26952)
- Prefix lengths for columns in `SPATIAL` indexes are no longer displayed in `SHOW CREATE TABLE` output. `mysqldump` uses that statement, so if a table with `SPATIAL` indexes containing prefixed columns is dumped and reloaded, the index is created with no prefixes. (The full column width of each column is indexed.) (Bug #26794)
- The output of `mysql --xml` and `mysqldump --xml` now includes a valid XML namespace. (Bug #25946)

- If you use SSL for a client connection, you can tell the client not to authenticate the server certificate by specifying neither `--ssl-ca` nor `--ssl-capath`. The server still verifies the client according to any applicable requirements established using `GRANT` statements for the client, and it still uses any `--ssl-ca/--ssl-capath` values that were passed to server at startup time. (Bug #25309)
- The syntax for index hints has been extended to enable explicit specification that the hint applies only to join processing. See [Index Hints](#).

This is a new fix for this issue, and replaces the fix made in MySQL 5.0.25 and reverted in 5.0.26. (Bug #21174)

- The `mysql_create_system_tables` script was removed because `mysql_install_db` no longer uses it.

Bugs Fixed

- **Important Note:** The parser accepted invalid code in SQL condition handlers, leading to server crashes or unexpected execution behavior in stored programs. Specifically, the parser permitted a condition handler to refer to labels for blocks that enclose the handler declaration. This was incorrect because block label scope does not include the code for handlers declared within the labeled block.

The parser now rejects this invalid construct, but if you perform a binary upgrade (without dumping and reloading your databases), existing handlers that contain the construct are still invalid and should be rewritten *even if they appear to function as you expect*.

To find affected handlers, use `mysqldump` to dump all stored procedures and functions, triggers, and events. Then attempt to reload them into an upgraded server. Handlers that contain illegal label references will be rejected.

For more information about condition handlers and writing them to avoid invalid jumps, see [DECLARE ... HANDLER Syntax](#). (Bug #26503)

- **MySQL Cluster:** NDB tables having `MEDIUMINT AUTO_INCREMENT` columns were not restored correctly by `ndb_restore`, causing spurious duplicate key errors. This issue did not affect `TINYINT`, `INT`, or `BIGINT` columns with `AUTO_INCREMENT`. (Bug #27775)
- **MySQL Cluster:** NDB tables with indexes whose names contained space characters were not restored correctly by `ndb_restore` (the index names were truncated). (Bug #27758)
- **MySQL Cluster:** Under certain rare circumstances performing a `DROP TABLE` or `TRUNCATE TABLE` on an NDB table could cause a node failure or forced cluster shutdown. (Bug #27581)
- **MySQL Cluster:** Memory usage of a `mysqld` process grew even while idle. (Bug #27560)
- **MySQL Cluster:** It was not possible to set `LockPagesInMainMemory` equal to 0. (Bug #27291)
- **MySQL Cluster:** A race condition could sometimes occur if the node acting as master failed while node IDs were still being allocated during startup. (Bug #27286)
- **MySQL Cluster:** When a data node was taking over as the master node, a race condition could sometimes occur as the node was assuming responsibility for handling of global checkpoints. (Bug #27283)
- **MySQL Cluster:** Error messages displayed when running in single user mode were inconsistent. (Bug #27021)
- **MySQL Cluster:** The failure of a data node while restarting could cause other data nodes to hang or crash. (Bug #27003)

- **MySQL Cluster:** On Solaris, the value of an NDB table column declared as `BIT(33)` was always displayed as `0`. (Bug #26986)
- **MySQL Cluster:** `mysqld` processes would sometimes crash under high load. (Bug #26825)
- **MySQL Cluster:** The output from `ndb_restore --print_data` was incorrect for a backup made of a database containing tables with `TINYINT` or `SMALLINT` columns. (Bug #26740)
- **MySQL Cluster:** In some cases, `AFTER UPDATE` and `AFTER DELETE` triggers on NDB tables that referenced subject table did not see the results of operation which caused invocation of the trigger, but rather saw the row as it was prior to the update or delete operation.

This was most noticeable when an update operation used a subquery to obtain the rows to be updated. An example would be `UPDATE tbl1 SET col2 = val1 WHERE tbl1.col1 IN (SELECT col3 FROM tbl2 WHERE c4 = val2)` where there was an `AFTER UPDATE` trigger on table `tbl1`. In such cases, the trigger failed to execute.

The problem occurred because the actual update or delete operations were deferred to be able to perform them later as one batch. The fix for this bug solves the problem by disabling this optimization for a given update or delete if the table has an `AFTER` trigger defined for this operation. (Bug #26242)

- **MySQL Cluster:** Condition pushdown did not work with prepared statements. (Bug #26225)
- **MySQL Cluster:** Joins on multiple tables containing `BLOB` columns could cause data nodes run out of memory, and to crash with the error `NdbObjectIdMap::expand unable to expand`. (Bug #26176)
- **MySQL Cluster:** After entering single user mode it was not possible to alter non-NDB tables on any SQL nodes other than the one having sole access to the cluster. (Bug #25275)
- **MySQL Cluster:** When a cluster data node suffered a “hard” failure (such as a power failure or loss of a network connection) TCP sockets to the missing node were maintained indefinitely. Now socket-based transporters check for a response and terminate the socket if there is no activity on the socket after 2 hours. (Bug #24793)
- **MySQL Cluster:** The management client command `node_id STATUS` displayed the message `Node node_id: not connected` when `node_id` was not the node ID of a data node.



Note

The `ALL STATUS` command in the cluster management client still displays status information for data nodes only. This is by design. See [Commands in the MySQL Cluster Management Client](#), for more information.

(Bug #21715)

- **MySQL Cluster:** Some values of `MaxNoOfTables` caused the error `Job buffer congestion` to occur. (Bug #19378)
- **MySQL Cluster:** When trying to create tables on an SQL node not connected to the cluster, a misleading error message `Table 'tbl_name' already exists` was generated. The error now generated is `Could not connect to storage engine`. (Bug #11217, Bug #18676)
- **Replication:** Out-of-memory errors were not reported. Now they are written to the error log. (Bug #26844)
- **Replication:** Improved out-of-memory detection when sending logs from a master server to slaves, and log a message when allocation fails. (Bug #26837)

- **Replication:** When `RAND()` was called multiple times inside a stored procedure, the server did not write the correct random seed values to the binary log, resulting in incorrect replication. (Bug #25543)
- **Replication:** `GRANT` statements were not replicated if the server was started with the `--replicate-ignore-table` or `--replicate-wild-ignore-table` option. (Bug #25482)
- **Replication:** Replication between master and slave would infinitely retry binary log transmission where the `max_allowed_packet` on the master was larger than that on the slave if the size of the transfer was between these two values. (Bug #23775)
- **Cluster Replication:** Some queries that updated multiple tables were not backed up correctly. (Bug #27748)
- **Cluster API:** Using `NdbBlob::writeData()` to write data in the middle of an existing blob value (that is, updating the value) could overwrite some data past the end of the data to be changed. (Bug #27018)
- **Cluster API:** After defining a delete operation (using `NdbOperation::deleteTuple()`) on a nonexistent primary key of a table having a `BLOB` or `TEXT` column, invoking `NdbTransaction::execute()` caused the calling application to enter an endless loop rather than raising an error.

This issue also affected `ndb_restore`; when restoring tables containing `BLOB` or `TEXT` columns, this could cause it to consume all available memory and then crash. (Bug #24028)

References: See also: Bug #27308, Bug #30177.

- Some equi-joins containing a `WHERE` clause that included a `NOT IN` subquery caused a server crash. (Bug #27870)
- `SELECT DISTINCT` could return incorrect results if the select list contained duplicated columns. (Bug #27659)
- With `NO_AUTO_VALUE_ON_ZERO` SQL mode enabled, `LOAD DATA` operations could assign incorrect `AUTO_INCREMENT` values. (Bug #27586)
- Incorrect results could be returned for some queries that contained a select list expression with `IN` or `BETWEEN` together with an `ORDER BY` or `GROUP BY` on the same expression using `NOT IN` or `NOT BETWEEN`. (Bug #27532)
- Evaluation of an `IN()` predicate containing a decimal-valued argument caused a server crash. (Bug #27513, Bug #27362, CVE-2007-2583)
- In out-of-memory conditions, the server might crash or otherwise not report an error to the Windows event log. (Bug #27490)
- Passing nested row expressions with different structures to an `IN` predicate caused a server crash. (Bug #27484)
- The `decimal.h` header file was incorrectly omitted from binary distributions. (Bug #27456)
- With `innodb_file_per_table` enabled, attempting to rename an `InnoDB` table to a nonexistent database caused the server to exit. (Bug #27381)
- A subquery could get incorrect values for references to outer query columns when it contained aggregate functions that were aggregated in outer context. (Bug #27321)
- The server did not shut down cleanly. (Bug #27310)

- In a view, a column that was defined using a [GEOMETRY](#) function was treated as having the [LONGBLOB](#) data type rather than the [GEOMETRY](#) type. (Bug #27300)
- Queries containing subqueries with [COUNT\(*\)](#) aggregated in an outer context returned incorrect results. This happened only if the subquery did not contain any references to outer columns. (Bug #27257)
- Use of an aggregate function from an outer context as an argument to [GROUP_CONCAT\(\)](#) caused a server crash. (Bug #27229)
- String truncation upon insertion into an integer or year column did not generate a warning (or an error in strict mode). (Bug #27176, Bug #26359)
- Storing [NULL](#) values in spatial fields caused excessive memory allocation and crashes on some systems. (Bug #27164)
- Row equalities in [WHERE](#) clauses could cause memory corruption. (Bug #27154)
- [GROUP BY](#) on a [ucs2](#) column caused a server crash when there was at least one empty string in the column. (Bug #27079)
- Duplicate members in [SET](#) or [ENUM](#) definitions were not detected. Now they result in a warning; if strict SQL mode is enabled, an error occurs instead. (Bug #27069)
- For [INSERT ... ON DUPLICATE KEY UPDATE](#) statements on tables containing [AUTO_INCREMENT](#) columns, [LAST_INSERT_ID\(\)](#) was reset to 0 if no rows were successfully inserted or changed. “Not changed” includes the case where a row was updated to its current values, but in that case, [LAST_INSERT_ID\(\)](#) should not be reset to 0. Now [LAST_INSERT_ID\(\)](#) is reset to 0 only if no rows were successfully inserted or touched, whether or not touched rows were changed. (Bug #27033)

References: See also: Bug #27210, Bug #27006. This issue is a regression of: Bug #19978.

- [mysql_install_db](#) could terminate with an error after failing to determine that a system table already existed. (Bug #27022)
- In a [MEMORY](#) table, using a [BTREE](#) index to scan for updatable rows could lead to an infinite loop. (Bug #26996)
- Invalid optimization of pushdown conditions for queries where an outer join was guaranteed to read only one row from the outer table led to results with too few rows. (Bug #26963)
- Windows binaries contained no debug symbol file. Now [.map](#) and [.pdb](#) files are included in 32-bit builds for [mysqld-nt.exe](#), [mysqld-debug.exe](#), and [mysqlmanager.exe](#). (Bug #26893)
- For [InnoDB](#) tables having a clustered index that began with a [CHAR](#) or [VARCHAR](#) column, deleting a record and then inserting another before the deleted record was purged could result in table corruption. (Bug #26835)
- Duplicates were not properly identified among (potentially) long strings used as arguments for [GROUP_CONCAT\(DISTINCT\)](#). (Bug #26815)
- [ALTER VIEW](#) requires the [CREATE VIEW](#) and [DROP](#) privileges for the view. However, if the view was created by another user, the server erroneously required the [SUPER](#) privilege. (Bug #26813)
- A result set column formed by concatenation of string literals was incomplete when the column was produced by a subquery in the [FROM](#) clause. (Bug #26738)
- When using the result of [SEC_TO_TIME\(\)](#) for time value greater than 24 hours in an [ORDER BY](#) clause, either directly or through a column alias, the rows were sorted incorrectly as strings. (Bug #26672)
- The range optimizer could cause the server to run out of memory. (Bug #26625)

- The range optimizer could consume a combinatorial amount of memory for certain classes of `WHERE` clauses. (Bug #26624)
- `mysqldump` could crash or exhibit incorrect behavior when some options were given very long values, such as `--fields-terminated-by="some very long string"`. The code has been cleaned up to remove a number of fixed-sized buffers and to be more careful about error conditions in memory allocation. (Bug #26346)
- If the server was started with `--skip-grant-tables`, selecting from `INFORMATION_SCHEMA` tables caused a server crash. (Bug #26285)
- For an `INSERT` statement that should fail due to a column with no default value not being assigned a value, the statement succeeded with no error if the column was assigned a value in an `ON DUPLICATE KEY UPDATE` clause, even if that clause was not used. (Bug #26261)
- The temporary file-creation code was cleaned up on Windows to improve server stability. (Bug #26233)
- For `MyISAM` tables, `COUNT(*)` could return an incorrect value if the `WHERE` clause compared an indexed `TEXT` column to the empty string (`' '`). This happened if the column contained empty strings and also strings starting with control characters such as tab or newline. (Bug #26231)
- For `INSERT INTO ... SELECT` where index searches used column prefixes, insert errors could occur when key value type conversion was done. (Bug #26207)
- For `DELETE FROM tbl_name ORDER BY col_name` (with no `WHERE` or `LIMIT` clause), the server did not check whether `col_name` was a valid column in the table. (Bug #26186)
- `REPAIR TABLE ... USE_FRM` with an `ARCHIVE` table deleted all records from the table. (Bug #26138)
- `mysqldump` crashed for `MERGE` tables if the `--complete-insert (-c)` option was given. (Bug #25993)
- Setting a column to `NOT NULL` with an `ON DELETE SET NULL` clause foreign key crashes the server. (Bug #25927)
- On Windows, debug builds of `mysqld` could fail with heap assertions. (Bug #25765)
- In certain situations, `MATCH ... AGAINST` returned false hits for `NULL` values produced by `LEFT JOIN` when no full-text index was available. (Bug #25729)
- `OPTIMIZE TABLE` might fail on Windows when it attempts to rename a temporary file to the original name if the original file had been opened, resulting in loss of the `.MYD` file. (Bug #25521)
- For `SHOW ENGINE INNODB STATUS`, the `LATEST DEADLOCK INFORMATION` was not always cleared properly. (Bug #25494)
- `mysql_stmt_fetch()` did an invalid memory deallocation when used with the embedded server. (Bug #25492)
- Difficult repair or optimization operations could cause an assertion failure, resulting in a server crash. (Bug #25289)
- Duplicate entries were not assessed correctly in a `MEMORY` table with a `BTREE` primary key on a `utf8 ENUM` column. (Bug #24985)
- Selecting the result of `AVG()` within a `UNION` could produce incorrect values. (Bug #24791)
- `MBROverlaps()` returned incorrect values in some cases. (Bug #24563)
- Increasing the width of a `DECIMAL` column could cause column values to be changed. (Bug #24558)

- A problem in handling of aggregate functions in subqueries caused predicates containing aggregate functions to be ignored during query execution. (Bug #24484)
- The test for the `MYSQL_OPT_SSL_VERIFY_SERVER_CERT` option for `mysql_options()` was performed incorrectly. Also changed as a result of this bug fix: The `arg` option for the `mysql_options()` C API function was changed from `char *` to `void *`. (Bug #24121)
- On Windows, debug builds of `mysqlbinlog` could fail with a memory error. (Bug #23736)
- The values displayed for the `InnoDB_row_lock_time`, `InnoDB_row_lock_time_avg`, and `InnoDB_row_lock_time_max` status variables were incorrect. (Bug #23666)
- `SHOW CREATE VIEW` qualified references to stored functions in the view definition with the function's database name, even when the database was the default database. This affected `mysqldump` (which uses `SHOW CREATE VIEW` to dump views) because the resulting dump file could not be used to reload the database into a different database. `SHOW CREATE VIEW` now suppresses the database name for references to stored functions in the default database. (Bug #23491)
- An `INTO OUTFILE` clause is permitted only for the final `SELECT` of a `UNION`, but this restriction was not being enforced correctly. (Bug #23345)
- With the `NO_AUTO_VALUE_ON_ZERO` SQL mode enabled, `LAST_INSERT_ID()` could return 0 after `INSERT ... ON DUPLICATE KEY UPDATE`. Additionally, the next rows inserted (by the same `INSERT`, or the following `INSERT` with or without `ON DUPLICATE KEY UPDATE`), would insert 0 for the auto-generated value if the value for the `AUTO_INCREMENT` column was `NULL` or missing. (Bug #23233)
- `SOUNDEX()` returned an invalid string for international characters in multibyte character sets. (Bug #22638)
- `COUNT(decimal_expr)` sometimes generated a spurious truncation warning. (Bug #21976)
- `InnoDB`: The first read statement, if served from the query cache, was not consistent with the `READ COMMITTED` isolation level. (Bug #21409)
- For a stored procedure containing a `SELECT` statement that used a complicated join with an `ON` expression, the expression could be ignored during re-execution of the procedure, yielding an incorrect result. (Bug #20492)
- In some cases, the optimizer preferred a range or full index scan access method over lookup access methods when the latter were much cheaper. (Bug #19372)
- Conversion of `DATETIME` values in numeric contexts sometimes did not produce a double (`YYYYMMDDHHMMSS.uuuuuu`) value. (Bug #16546)

Changes in MySQL Enterprise 5.0.38 [MRU] (2007-03-20)

This is a *Monthly Rapid Update* release of the MySQL Enterprise Server 5.0.

This section documents all changes and bug fixes that have been applied since the last MySQL Enterprise Server release (5.0.36).

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- The server now includes a timestamp in error messages that are logged as a result of unhandled signals (such as `mysqld got signal 11` messages). (Bug #24878)

- Added the `--secure-file-priv` option for `mysqld`, which limits the effect of the `LOAD_FILE()` function and the `LOAD DATA` and `SELECT ... INTO OUTFILE` statements to work only with files in a given directory. (Bug #18628)
- Added the read-only `hostname` system variable, which the server sets at startup to the server host name.
- To satisfy different user requirements, we provide several servers. `mysqld` is an optimized server that is a smaller, faster binary. Each package now also includes `mysqld-debug`, which is compiled with debugging support but is otherwise configured identically to the nondebug server.

Bugs Fixed

- **Incompatible Change:** `INSERT DELAYED` statements are not supported for `MERGE` tables, but the `MERGE` storage engine was not rejecting such statements, resulting in table corruption. Applications previously using `INSERT DELAYED` into `MERGE` table will break when upgrading to versions with this fix. To avoid the problem, remove `DELAYED` from such statements. (Bug #26464)
- **MySQL Cluster:** An inadvertent use of unaligned data caused `ndb_restore` to fail on some 64-bit platforms, including Sparc and Itanium-2. (Bug #26739)
- **MySQL Cluster:** An infinite loop in an internal logging function could cause trace logs to fill up with `Unknown Signal type` error messages and thus grow to unreasonable sizes. (Bug #26720)
- **MySQL Cluster:** An invalid pointer was returned following a `FSCLOSECONF` signal when accessing the REDO logs during a node restart or system restart. (Bug #26515)
- **MySQL Cluster:** The failure of a data node when restarting it with `--initial` could lead to failures of subsequent data node restarts. (Bug #26481)
- **MySQL Cluster:** Takeover for local checkpointing due to multiple failures of master nodes was sometimes incorrectly handled. (Bug #26457)
- **MySQL Cluster:** The `LockPagesInMainMemory` parameter was not read until after distributed communication had already started between cluster nodes. When the value of this parameter was `1`, this could sometimes result in data node failure due to missed heartbeats. (Bug #26454)
- **MySQL Cluster:** Under some circumstances, following the restart of a management node, all data nodes would connect to it normally, but some of them subsequently failed to log any events to the management node. (Bug #26293)
- **MySQL Cluster:** The message `Error 0 in readAutoIncrementValue(): no Error` was written to the error log whenever `SHOW TABLE STATUS` was performed on a Cluster table that did not have an `AUTO_INCREMENT` column. (Bug #21033)
- **Replication:** A multiple-row delayed insert with an auto-increment column could cause duplicate entries to be created on the slave in a replication environment. (Bug #26116, Bug #25507)
- **Replication:** Duplicating the usage of a user variable in a stored procedure or trigger would not be replicated correctly to the slave. (Bug #25167)
- **Replication:** `DROP TRIGGER` statements would not be filtered on the slave when using the `replication-wild-do-table` option. (Bug #24478)
- **Replication:** For `INSERT ... ON DUPLICATE KEY UPDATE` statements where some `AUTO_INCREMENT` values were generated automatically for inserts and some rows were updated, one auto-generated value was lost per updated row, leading to faster exhaustion of the range of the `AUTO_INCREMENT` column.

Because the original problem can affect replication (different values on master and slave), it is recommended that the master and its slaves be upgraded to the current version. (Bug #24432)

- **Replication:** Loading data using `LOAD DATA INFILE` may not replicate correctly (due to character set incompatibilities) if the `character_set_database` variable is set before the data is loaded. (Bug #15126)
- **Replication:** User defined variables used within stored procedures and triggers are not replicated correctly when operating in statement-based replication mode. (Bug #14914, Bug #20141)
- `SELECT ... INTO OUTFILE` with a long `FIELDS ENCLOSED BY` value could crash the server. (Bug #27231)
- An `INSERT ... ON DUPLICATE KEY UPDATE` statement might modify values in a table but not flush affected data from the query cache, causing subsequent selects to return stale results. This made the combination of query cache plus `ON DUPLICATE KEY UPDATE` very unreliable. (Bug #27210)

References: See also: Bug #27006, Bug #27033. This issue is a regression of: Bug #19978.

- For `MERGE` tables defined on underlying tables that contained a short `VARCHAR` column (shorter than four characters), using `ALTER TABLE` on at least one but not all of the underlying tables caused the table definitions to be considered different from that of the `MERGE` table, even if the `ALTER TABLE` did not change the definition. (Bug #26881)
- Use of a subquery containing `GROUP BY` and `WITH ROLLUP` caused a server crash. (Bug #26830)
- Added support for `--debugger=dbx` for `mysql-test-run.pl` and added support for `--debugger=devenv`, `--debugger=DevEnv`, and `--debugger=/path/to/devenv`. (Bug #26792)
- SSL connections failed on Windows. (Bug #26678)
- Use of a subquery containing a `UNION` with an invalid `ORDER BY` clause caused a server crash. (Bug #26661)
- In some error messages, inconsistent format specifiers were used for the translations in different languages. `comp_err` (the error message compiler) now checks for mismatches. (Bug #26571)
- Views that used a scalar correlated subquery returned incorrect results. (Bug #26560)
- `UNHEX() IS NULL` comparisons failed when `UNHEX()` returned `NULL`. (Bug #26537)
- On 64-bit Windows, large timestamp values could be handled incorrectly. (Bug #26536)
- For some values of the position argument, the `INSERT()` function could insert a NUL byte into the result. (Bug #26281)
- `INSERT DELAYED` statements inserted incorrect values into `BIT` columns. (Bug #26238)
- `BENCHMARK()` did not work correctly for expressions that produced a `DECIMAL` result. (Bug #26093)
- `LOAD DATA INFILE` sent an okay to the client before writing the binary log and committing the changes to the table had finished, thus violating ACID requirements. (Bug #26050)
- `X() IS NULL` and `Y() IS NULL` comparisons failed when `X()` and `Y()` returned `NULL`. (Bug #26038)
- Indexes on `TEXT` columns were ignored when `ref` accesses were evaluated. (Bug #25971)
- If a thread previously serviced a connection that was killed, excessive memory and CPU use by the thread occurred if it later serviced a connection that had to wait for a table lock. (Bug #25966)

- `VIEW` restrictions were applied to `SELECT` statements after a `CREATE VIEW` statement failed, as though the `CREATE` had succeeded. (Bug #25897)
- Several deficiencies in resolution of column names for `INSERT ... SELECT` statements were corrected. (Bug #25831)
- Inserting `utf8` data into a `TEXT` column that used a single-byte character set could result in spurious warnings about truncated data. (Bug #25815)
- In certain cases it could happen that deleting a row corrupted an `RTREE` index. This affected indexes on spatial columns. (Bug #25673)
- Expressions involving `SUM()`, when used in an `ORDER BY` clause, could lead to out-of-order results. (Bug #25376)
- Use of a `GROUP BY` clause that referred to a stored function result together with `WITH ROLLUP` caused incorrect results. (Bug #25373)
- A stored procedure that made use of cursors failed when the procedure was invoked from a stored function. (Bug #25345)
- On Windows, the server exhibited a file-handle leak after reaching the limit on the number of open file descriptors. (Bug #25222)
- The `REPEAT()` function did not permit a column name as the `count` parameter. (Bug #25197)
- A reference to a nonexistent column in the `ORDER BY` clause of an `UPDATE ... ORDER BY` statement could cause a server crash. (Bug #25126)
- A view on a join is insertable for `INSERT` statements that store values into only one table of the join. However, inserts were being rejected if the inserted-into table was used in a self-join because MySQL incorrectly was considering the insert to modify multiple tables of the view. (Bug #25122)
- MySQL would not compile when configured using `--without-query-cache`. (Bug #25075)
- `IF(expr, unsigned_expr, unsigned_expr)` was evaluated to a signed result, not unsigned. This has been corrected. The fix also affects constructs of the form `IS [NOT] {TRUE|FALSE}`, which were transformed internally into `IF()` expressions that evaluated to a signed result.

For existing views that were defined using `IS [NOT] {TRUE|FALSE}` constructs, there is a related implication. The definitions of such views were stored using the `IF()` expression, not the original construct. This is manifest in that `SHOW CREATE VIEW` shows the transformed `IF()` expression, not the original one. Existing views will evaluate correctly after the fix, but if you want `SHOW CREATE VIEW` to display the original construct, you must drop the view and re-create it using its original definition. New views will retain the construct in their definition. (Bug #24532)

- A user-defined variable could be assigned an incorrect value if a temporary table was employed in obtaining the result of the query used to determine its value. (Bug #24010)
- Queries that used a temporary table for the outer query when evaluating a correlated subquery could return incorrect results. (Bug #23800)
- When using certain server SQL modes, the `mysql.proc` table was not created by `mysql_install_db`. (Bug #23669)
- `DOUBLE` values such as `20070202191048.000000` were being treated as illegal arguments by `WEEK()`. (Bug #23616)

- The server could crash if two or more threads initiated query cache resize operation at moments very close in time. (Bug #23527)
- `NOW()` returned the wrong value in statements executed at server startup with the `--init-file` option. (Bug #23240)
- When nesting stored procedures within a trigger on a table, a false dependency error was thrown when one of the nested procedures contained a `DROP TABLE` statement. (Bug #22580)
- Instance Manager did not remove the angel PID file on a clean shutdown. (Bug #22511)
- `EXPLAIN EXTENDED` did not show `WHERE` conditions that were optimized away. (Bug #22331)
- `IN ((subquery))`, `IN (((subquery)))`, and so forth, are equivalent to `IN (subquery)`, which is always interpreted as a table subquery (so that it is permitted to return more than one row). MySQL was treating the “over-parenthesized” subquery as a single-row subquery and rejecting it if it returned more than one row. This bug primarily affected automatically generated code (such as queries generated by Hibernate), because humans rarely write the over-parenthesized forms. (Bug #21904)
- An `INSERT` trigger invoking a stored routine that inserted into a table other than the one on which the trigger was defined failed with `Table '...' doesn't exist` referring to the second table when attempting to delete records from the first table. (Bug #21825)
- When a stored routine attempted to execute a statement accessing a nonexistent table, the error was not caught by the routine's exception handler. (Bug #20713, Bug #8407)
- The conditions checked by the optimizer to permit use of indexes in `IN` predicate calculations were unnecessarily tight and were relaxed. (Bug #20420)
- When a `TIME_FORMAT()` expression was used as a column in a `GROUP BY` clause, the expression result was truncated. (Bug #20293)
- The creation of MySQL system tables was not checked for by `mysql-test-run.pl`. (Bug #20166)
- For index reads, the `BLACKHOLE` engine did not return end-of-file (which it must because `BLACKHOLE` tables contain no rows), causing some queries to crash. (Bug #19717)
- For `expr IN(value_list)`, the result could be incorrect if `BIGINT UNSIGNED` values were used for `expr` or in the value list. (Bug #19342)
- When attempting to call a stored procedure creating a table from a trigger on a table `tbl` in a database `db`, the trigger failed with `ERROR 1146 (42S02): Table 'db.tbl' doesn't exist`. However, the actual reason that such a trigger fails is due to the fact that `CREATE TABLE` causes an implicit `COMMIT`, and so a trigger cannot invoke a stored routine containing this statement. A trigger which does so now fails with `ERROR 1422 (HY000): Explicit or implicit commit is not permitted in stored function or trigger`, which makes clear the reason for the trigger's failure. (Bug #18914)
- The update columns for `INSERT ... SELECT ... ON DUPLICATE KEY UPDATE` could be assigned incorrect values if a temporary table was used to evaluate the `SELECT`. (Bug #16630)
- For `SUBSTRING()` evaluation using a temporary table, when `SUBSTRING()` was used on a `LONGTEXT` column, the `max_length` metadata value of the result was incorrectly calculated and set to 0. Consequently, an empty string was returned instead of the correct result. (Bug #15757)
- Local variables in stored routines or triggers, when declared as the `BIT` type, were interpreted as strings. (Bug #12976)
- `CONNECTION` is no longer treated as a reserved word. (Bug #12204)

Changes in MySQL Community Server 5.0.37 (2007-02-27)

This is a bugfix release for the current MySQL Community Server production release family. It replaces MySQL 5.0.33.

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- **Incompatible Change; MySQL Cluster:** The `LockPagesInMainMemory` configuration parameter has changed its type and possible values.



Important

The values `true` and `false` are no longer accepted for this parameter. If you were using this parameter and had it set to `false` in a previous release, you must change it to `0`. If you had this parameter set to `true`, you should instead use `1` to obtain the same behavior as previously, or `2` to take advantage of new functionality introduced with this release, as described in the section cited above.

(Bug #25686)

- **Incompatible Change:** Previously, the `DATE_FORMAT()` function returned a binary string. Now it returns a string with a character set and collation given by `character_set_connection` and `collation_connection` so that it can return month and weekday names containing non-ASCII characters. (Bug #22646)
 - **Important Change:** When using a `MERGE` table, the definition of the table and the underlying `MyISAM` tables are checked each time the tables are opened for access (including any `SELECT` or `INSERT` statement). Each table is compared for column order, types, sizes, and associated indexes. If there is a difference in any one of the tables, the statement will fail.
 - Added the `Uptime_since_flush_status` status variable, which indicates the number of seconds since the most recent `FLUSH STATUS` statement. (Community contribution by Jeremy Cole) (Bug #24822)
 - Added the `SHOW PROFILES` and `SHOW PROFILE` statements to display statement profile data, and the accompanying `INFORMATION_SCHEMA.PROFILING` table. Profiling is controlled using the `profiling` and `profiling_history_size` session variables. see [SHOW PROFILES Syntax](#), and [The INFORMATION_SCHEMA PROFILING Table](#). (Community contribution by Jeremy Cole)
- The profiling feature is enabled using the `--enable-community-features` and `--enable-profiling` options to `configure`. These options are enabled by default; to disable them, use `--disable-community-features` and `--disable-profiling`. (Bug #24795)
- The `localhost` anonymous user account created during MySQL installation on Windows now has no global privileges. Formerly this account had all global privileges. For operations that require global privileges, the `root` account can be used instead. (Bug #24496)
 - The `--skip-thread-priority` option now is enabled by default for binary Mac OS X distributions. Use of thread priorities degrades performance on Mac OS X. (Bug #18526)
 - This is the last version for which MySQL-Max RPM distributions are available. (This change was already made for non-RPM binary distributions in 5.0.27.)

- The bundled yaSSL library was upgraded to version 1.5.8.
- Added the `--disable-grant-options` option to `configure`. If `configure` is run with this option, the `--bootstrap`, `--skip-grant-tables`, and `--init-file` options for `mysqld` are disabled and cannot be used. For Windows, the `configure.js` script recognizes the `DISABLE_GRANT_OPTIONS` flag, which has the same effect.

Bugs Fixed

- **Security Fix:** Using an `INFORMATION_SCHEMA` table with `ORDER BY` in a subquery could cause a server crash.

We would like to thank Oren Isacson of Flowgate Security Consulting and Stefan Streichsbier of SEC Consult for informing us of this problem. (Bug #24630, Bug #26556, CVE-2007-1420)

- **Incompatible Change:** For `ENUM` columns that had enumeration values containing commas, the commas were mapped to `0xff` internally. However, this rendered the commas indistinguishable from true `0xff` characters in the values. This no longer occurs. However, the fix requires that you dump and reload any tables that have `ENUM` columns containing any true `0xff` values. Dump the tables using `mysqldump` with the current server before upgrading from a version of MySQL 5.0 older than 5.0.36 to version 5.0.36 or newer. (Bug #24660)
- **MySQL Cluster; Partitioning:** A query with an `IN` clause against an `NDB` table employing explicit user-defined partitioning did not always return all matching rows. (Bug #25821)
- **MySQL Cluster:** It was not possible to create an `NDB` table with a key on two `VARCHAR` columns where both columns had a storage length in excess of 256. (Bug #25746)
- **MySQL Cluster:** Hosts in clusters with large numbers of nodes could experience excessive CPU usage while obtaining configuration data. (Bug #25711)
- **MySQL Cluster:** In some circumstances, shutting down the cluster could cause connected `mysqld` processes to crash. (Bug #25668)
- **MySQL Cluster:** Memory allocations for `TEXT` columns were calculated incorrectly, resulting in space being wasted and other issues. (Bug #25562)
- **MySQL Cluster:** The failure of a master node during a node restart could lead to a resource leak, causing later node failures. (Bug #25554)
- **MySQL Cluster:** An `UPDATE` using an `IN` clause on an `NDB` table on which there was a trigger caused `mysqld` to crash. (Bug #25522)
- **MySQL Cluster:** A node shutdown occurred if the master failed during a commit. (Bug #25364)
- **MySQL Cluster:** Creating a nonunique index with the `USING HASH` clause silently created an ordered index instead of issuing a warning. (Bug #24820)
- **MySQL Cluster:** The `ndb_size.tmp1` file (necessary for using the `ndb_size.pl` script) was missing from binary distributions. (Bug #24191)
- **MySQL Cluster:** When a data node was shut down using the management client `STOP` command, a connection event (`NDB_LE_Connected`) was logged instead of a disconnection event (`NDB_LE_Disconnected`). (Bug #22773)
- **MySQL Cluster:** The management server did not handle logging of node shutdown events correctly in certain cases. (Bug #22013)

- **MySQL Cluster:** `SELECT` statements with a `BLOB` or `TEXT` column in the selected column list and a `WHERE` condition including a primary key lookup on a `VARCHAR` primary key produced empty result sets. (Bug #19956)
- **Replication:** When `SET PASSWORD` was written to the binary log, double quotation marks were included in the statement. If the slave was running in with the server SQL mode set to `ANSI_QUOTES`, then the event failed, which halted the replication process. (Bug #24158)
- **Replication:** A stored procedure, executed from a connection using a binary character set, and which wrote multibyte data, would write incorrectly escaped entries to the binary log. This caused syntax errors, and caused replication to fail. (Bug #23619, Bug #24492)
- **Replication:** Changes to the `lc_time_names` system variable were not replicated. (Bug #22645)
- **Replication:** For `SET`, `SELECT`, and `DO` statements that invoked a stored function from a database other than the default database, the function invocation could fail to be replicated. (Bug #19725)
- **Replication:** If a slave server closed its relay log (for example, due to an error during log rotation), the I/O thread did not recognize this and still tried to write to the log, causing a server crash. (Bug #10798)
- **Cluster API:** Deletion of an `Ndb_cluster_connection` object took a very long time. (Bug #25487)
- **Cluster API:** Invoking the `NdbTransaction::execute()` method using execution type `Commit` and abort option `AO_IgnoreError` could lead to a crash of the transaction coordinator (DBTC). (Bug #25090)
- **Cluster API:** A unique index lookup on a nonexistent tuple could lead to a data node timeout (error 4012). (Bug #25059)
- **Cluster API:** `libndbclient.so` was not versioned. (Bug #13522)
- Using `ORDER BY` or `GROUP BY` could yield different results when selecting from a view and selecting from the underlying table. (Bug #26209)
- `DISTINCT` queries that were executed using a loose scan for an `InnoDB` table that had been emptied caused a server crash. (Bug #26159)
- A `WHERE` clause that used `BETWEEN` for `DATETIME` values could be treated differently for a `SELECT` and a view defined as that `SELECT`. (Bug #26124)
- Collation for `LEFT JOIN` comparisons could be evaluated incorrectly, leading to improper query results. (Bug #26017)
- The `WITH CHECK OPTION` clause for views was ignored for updates of multiple-table views when the updates could not be performed on fly and the rows to update had to be put into temporary tables first. (Bug #25931)
- `LOAD DATA INFILE` did not work with pipes. (Bug #25807)
- The `SEC_TO_TIME()` and `QUARTER()` functions sometimes did not handle `NULL` values correctly. (Bug #25643)
- The `InnoDB` parser sometimes did not account for null bytes, causing spurious failure of some queries. (Bug #25596)
- View definitions that used the `!` operator were treated as containing the `NOT` operator, which has a different precedence and can produce different results. (Bug #25580)
- An error in the name resolution of nested `JOIN ... USING` constructs was corrected. (Bug #25575)

- `GROUP BY` and `DISTINCT` did not group `NULL` values for columns that have a `UNIQUE` index. . (Bug #25551)
- The `--with-readline` option for `configure` did not work for commercial source packages, but no error message was printed to that effect. Now a message is printed. (Bug #25530)
- `mysql_stmt_fetch()` did an invalid memory deallocation when used with the embedded server. (Bug #25492)
- Referencing an ambiguous column alias in an expression in the `ORDER BY` clause of a query caused the server to crash. (Bug #25427)
- A yaSSL program named `test` was installed, causing conflicts with the `test` system utility. It is no longer installed. (Bug #25417)
- For a `UNIQUE` index containing many `NULL` values, the optimizer would prefer the index for `col IS NULL` conditions over other more selective indexes. . (Bug #25407)
- An `AFTER UPDATE` trigger on an `InnoDB` table with a composite primary key caused the server to crash. (Bug #25398)
- Passing a `NULL` value to a user-defined function from within a stored procedure crashes the server. (Bug #25382)
- `percona` crashed on some platforms due to failure to handle a `NULL` pointer. (Bug #25344)
- `mysql.server stop` timed out too quickly (35 seconds) waiting for the server to exit. Now it waits up to 15 minutes, to ensure that the server exits. (Bug #25341)
- A query that contained an `EXIST` subquery with a `UNION` over correlated and uncorrelated `SELECT` queries could cause the server to crash. (Bug #25219)
- `mysql_kill()` caused a server crash when used on an SSL connection. (Bug #25203)
- yaSSL was sensitive to the presence of whitespace at the ends of lines in PEM-encoded certificates, causing a server crash. (Bug #25189)
- A query with `ORDER BY` and `GROUP BY` clauses where the `ORDER BY` clause had more elements than the `GROUP BY` clause caused a memory overrun leading to a crash of the server. (Bug #25172)
- Use of `ON DUPLICATE KEY UPDATE` defeated the usual restriction against inserting into a join-based view unless only one of the underlying tables is used. (Bug #25123)
- Using a view in combination with a `USING` clause caused column aliases to be ignored. (Bug #25106)
- A multiple-table `DELETE QUICK` could sometimes cause one of the affected tables to become corrupted. (Bug #25048)
- `ALTER TABLE ... ENABLE KEYS` acquired a global lock, preventing concurrent execution of other statements that use tables. . (Bug #25044)
- An assertion failed incorrectly for prepared statements that contained a single-row uncorrelated subquery that was used as an argument of the `IS NULL` predicate. (Bug #25027)
- A return value of `-1` from user-defined handlers was not handled well and could result in conflicts with server code. (Bug #24987)
- Accessing a fixed record format table with a crashed key definition results in server/`myisamchk` segmentation fault. (Bug #24855)

- `mysqld_multi` and `mysqlaccess` looked for option files in `/etc` even if the `--sysconfdir` option for `configure` had been given to specify a different directory. (Bug #24780)
- If there was insufficient memory available to `mysqld`, this could sometimes cause the server to hang during startup. (Bug #24751)
- Optimizations that are legal only for subqueries without tables and `WHERE` conditions were applied for any subquery without tables. (Bug #24670)
- If an `ORDER BY` or `GROUP BY` list included a constant expression being optimized away and, at the same time, containing single-row subselects that returned more than one row, no error was reported. If a query required sorting by expressions containing single-row subselects that returned more than one row, execution of the query could cause a server crash. (Bug #24653)
- For `ALTER TABLE`, using `ORDER BY expression` could cause a server crash. Now the `ORDER BY` clause permits only column names to be specified as sort criteria (which was the only documented syntax, anyway). (Bug #24562)
- A workaround was implemented to avoid a race condition in the NPTL `pthread_exit()` implementation. (Bug #24507)
- `mysqltest` crashed with a stack overflow. (Bug #24498)
- Within stored routines or prepared statements, inconsistent results occurred with multiple use of `INSERT ... SELECT ... ON DUPLICATE KEY UPDATE` when the `ON DUPLICATE KEY UPDATE` clause erroneously tried to assign a value to a column mentioned only in its `SELECT` part. (Bug #24491)
- Expressions of the form `(a, b) IN (SELECT a, MIN(b) FROM t GROUP BY a)` could produce incorrect results when column `a` of table `t` contained `NULL` values while column `b` did not. (Bug #24420)
- If a prepared statement accessed a view, access to the tables listed in the query after that view was checked in the security context of the view. (Bug #24404)
- Attempts to access a `MyISAM` table with a corrupt column definition caused a server crash. (Bug #24401)
- When opening a corrupted `.frm` file during a query, the server crashes. (Bug #24358)
- Some joins in which one of the joined tables was a view could return erroneous results or crash the server. (Bug #24345)
- A view was not handled correctly if the `SELECT` part contained “\z”. (Bug #24293)
- A query using `WHERE unsigned_column NOT IN ('negative_value')` could cause the server to crash. (Bug #24261)
- Expressions of the form `(a, b) IN (SELECT c, d ...)` could produce incorrect results if `a`, `b`, or both were `NULL`. (Bug #24127)
- A `FETCH` statement using a cursor on a table which was not in the table cache could sometimes cause the server to crash. (Bug #24117)
- Queries that evaluate `NULL IN (SELECT ... UNION SELECT ...)` could produce an incorrect result (`FALSE` instead of `NULL`). (Bug #24085)
- Hebrew-to-Unicode conversion failed for some characters. Definitions for the following Hebrew characters (as specified by the ISO/IEC 8859-8:1999) were added: LEFT-TO-RIGHT MARK (LRM), RIGHT-TO-LEFT MARK (RLM) (Bug #24037)

- Some `UPDATE` statements were slower than in previous versions when the search key could not be converted to a valid value for the type of the search column. (Bug #24035)
- `ISNULL(DATE(NULL))` and `ISNULL(CAST(NULL AS DATE))` erroneously returned false. (Bug #23938)
- Within a stored routine, accessing a declared routine variable with `PROCEDURE ANALYSE()` caused a server crash. (Bug #23782)
- When reading from the standard input on Windows, `mysqlbinlog` opened the input in text mode rather than binary mode and consequently misinterpreted some characters such as **Control+Z**. (Bug #23735)
- `OPTIMIZE TABLE` tried to sort R-tree indexes such as spatial indexes, although this is not possible (see [OPTIMIZE TABLE Syntax](#)). (Bug #23578)
- For an InnoDB table with any `ON DELETE` trigger, `TRUNCATE TABLE` mapped to `DELETE` and activated triggers. Now a fast truncation occurs and triggers are not activated. . (Bug #23556)
- The row count for MyISAM tables was not updated properly, causing `SHOW TABLE STATUS` to report incorrect values. (Bug #23526)
- User-defined variables could consume excess memory, leading to a crash caused by the exhaustion of resources available to the `MEMORY` storage engine, due to the fact that this engine is used by MySQL for variable storage and intermediate results of `GROUP BY` queries. Where `SET` had been used, such a condition could instead give rise to the misleading error message `You may only use constant expressions with SET`, rather than `Out of memory (Needed NNNNNN bytes)`. (Bug #23443)
- With `ONLY_FULL_GROUP_BY` enabled, the server was too strict: Some expressions involving only aggregate values were rejected as nonaggregate (for example, `MAX(a) - MIN(a)`). (Bug #23417)
- The arguments to the `ENCODE()` and the `DECODE()` functions were not printed correctly, causing problems in the output of `EXPLAIN EXTENDED` and in view definitions. (Bug #23409)
- A table created with the `ROW_FORMAT = FIXED` table option lost that option if an index was added or dropped with `CREATE INDEX` or `DROP INDEX`. (Bug #23404)
- A deadlock could occur, with the server hanging on `Closing tables`, with a sufficient number of concurrent `INSERT DELAYED`, `FLUSH TABLES`, and `ALTER TABLE` operations. (Bug #23312)
- Some queries against `INFORMATION_SCHEMA` that used subqueries failed. . (Bug #23299)
- `readline` detection did not work correctly on NetBSD. (Bug #23293)
- If there was insufficient memory to store or update a blob record in a MyISAM table then the table will be marked as crashed. (Bug #23196)
- `LAST_INSERT_ID()` was not reset to 0 if `INSERT ... SELECT` inserted no rows. (Bug #23170)
- A compressed MyISAM table that became corrupted could crash `myisamchk` and possibly the MySQL Server. (Bug #23139)
- The number of `setsockopt()` calls performed for reads and writes to the network socket was reduced to decrease system call overhead. (Bug #22943)
- `mysql_upgrade` failed when called with a `--basedir` path name containing spaces. (Bug #22801)
- `SET lc_time_names = value` permitted only exact literal values, not expression values. (Bug #22647)
- The `STDDEV()` function returned a positive value for data sets consisting of a single value. (Bug #22555)

- Storing values specified as hexadecimal values 64 or more bits long in `BIT(64)`, `BIGINT`, or `BIGINT UNSIGNED` columns did not raise any warning or error if the value was out of range. (Bug #22533)
- `SHOW COLUMNS` reported some `NOT NULL` columns as `NULL`. (Bug #22377)
- Type conversion errors during formation of index search conditions were not correctly checked, leading to incorrect query results. (Bug #22344)
- Changing the value of `MI_KEY_BLOCK_LENGTH` in `myisam.h` and recompiling MySQL resulted in a `myisamchk` that saw existing `MyISAM` tables as corrupt. (Bug #22119)
- A crash of the MySQL Server could occur when unpacking a `BLOB` column from a row in a corrupted `MyISAM` table. This could happen when trying to repair a table using either `REPAIR TABLE` or `myisamchk`; it could also happen when trying to access such a “broken” row using statements like `SELECT` if the table was not marked as crashed. (Bug #22053)
- The code for generating `USE` statements for binary logging of `CREATE PROCEDURE` statements resulted in confusing output from `mysqlbinlog` for `DROP PROCEDURE` statements. (Bug #22043)
- For the `IF()` and `COALESCE()` function and `CASE` expressions, large unsigned integer values could be mishandled and result in warnings. (Bug #22026)
- SSL connections could hang at connection shutdown. (Bug #21781, Bug #24148)
- The `FEDERATED` storage engine did not support the `euckr` character set. (Bug #21556)
- When updating a table that used a `JOIN` of the table itself (for example, when building trees) and the table was modified on one side of the expression, the table would either be reported as crashed or the wrong rows in the table would be updated. (Bug #21310)
- `mysqld_error.h` was not installed when only the client libraries were built. (Bug #21265)
- `InnoDB`: During a restart of the MySQL Server that followed the creation of a temporary table using the `InnoDB` storage engine, MySQL failed to clean up in such a way that `InnoDB` still attempted to find the files associated with such tables. (Bug #20867)
- Inserting `DEFAULT` into a column with no default value could result in garbage in the column. Now the same result occurs as when inserting `NULL` into a `NOT NULL` column. (Bug #20691)
- A stored routine containing semicolon in its body could not be reloaded from a dump of a binary log. (Bug #20396)
- `SELECT ... FOR UPDATE`, `SELECT ... LOCK IN SHARE MODE`, `DELETE`, and `UPDATE` statements executed using a full table scan were not releasing locks on rows that did not satisfy the `WHERE` condition. (Bug #20390)
- On Windows, if the server was installed as a service, it did not auto-detect the location of the data directory. (Bug #20376)
- The `BUILD/check-cpu` script did not recognize Celeron processors. (Bug #20061)
- If a duplicate key value was present in the table, `INSERT ... ON DUPLICATE KEY UPDATE` reported a row count indicating that a record was updated, even when no record actually changed due to the old and new values being the same. Now it reports a row count of zero. (Bug #19978)

References: See also: Bug #27006, Bug #27033, Bug #27210.

- `ORDER BY` values of the `DOUBLE` or `DECIMAL` types could change the result returned by a query. (Bug #19690)

- The `readline` library wrote to uninitialized memory, causing `mysql` to crash. (Bug #19474)
- `mysqltest` incorrectly tried to retrieve result sets for some queries where no result set was available. (Bug #19410)
- Use of already freed memory caused SSL connections to hang forever. (Bug #19209)
- Some `CASE` statements inside stored routines could lead to excessive resource usage or a crash of the server. (Bug #19194, Bug #24854)
- Instance Manager could crash during shutdown. (Bug #19044)
- The server might fail to use an appropriate index for `DELETE` when `ORDER BY`, `LIMIT`, and a nonrestricting `WHERE` are present. (Bug #17711)
- No warning was issued for use of the `DATA DIRECTORY` or `INDEX DIRECTORY` table options on a platform that does not support them. (Bug #17498)
- The `FEDERATED` storage engine did not support the `utf8` character set. (Bug #17044)
- The optimizer removes expressions from `GROUP BY` and `DISTINCT` clauses if they happen to participate in `expression = constant` predicates of the `WHERE` clause, the idea being that, if the expression is equal to a constant, then it cannot take on multiple values. However, for predicates where the expression and the constant item are of different result types (for example, when a string column is compared to 0), this is not valid, and can lead to invalid results in such cases. The optimizer now performs an additional check of the result types of the expression and the constant; if their types differ, then the expression is not removed from the `GROUP BY` list. (Bug #15881)
- When a prepared statement failed during the prepare operation, the error code was not cleared when it was reused, even if the subsequent use was successful. (Bug #15518)
- Dropping a user-defined function sometimes did not remove the UDF entry from the `mysql.proc` table. (Bug #15439)
- Inserting a row into a table without specifying a value for a `BINARY(N) NOT NULL` column caused the column to be set to spaces, not zeros. (Bug #14171)
- On Windows, the `SLEEP()` function could sleep too long, especially after a change to the system clock. (Bug #14094, Bug #24686, Bug #17635)
- `mysqldump --order-by-primary` failed if the primary key name was an identifier that required quoting. (Bug #13926)
- To enable installation of MySQL RPMs on Linux systems running RHEL 4 (which includes SE-Linux) additional information was provided to specify some actions that are permitted to the MySQL binaries. (Bug #12676)
- The presence of `ORDER BY` in a view definition prevented the `MERGE` algorithm from being used to resolve the view even if nothing else in the definition required the `TEMPTABLE` algorithm. (Bug #12122)
- The internal functions for table preparation, creation, and alteration were not re-execution friendly, causing problems in code that: repeatedly altered a table; repeatedly created and dropped a table; opened and closed a cursor on a table, altered the table, and then reopened the cursor; used `ALTER TABLE` to change a table's current `AUTO_INCREMENT` value; created indexes on `utf8` columns.

Re-execution of `CREATE DATABASE`, `CREATE TABLE`, and `ALTER TABLE` statements in stored routines or as prepared statements also caused incorrect results or crashes. (Bug #4968, Bug #6895, Bug #19182, Bug #19733, Bug #22060, Bug #24879)

Changes in MySQL Enterprise 5.0.36sp1 [QSP] (2007-04-12)

This is a *Service Pack* release of the MySQL Enterprise Server 5.0.

This section documents all changes and bug fixes that have been applied since the last MySQL Enterprise Server release (5.0.36).

Bugs Fixed

- `SELECT ... INTO OUTFILE` with a long `FIELDS ENCLOSED BY` value could crash the server. (Bug #27231)
- For `MERGE` tables defined on underlying tables that contained a short `VARCHAR` column (shorter than four characters), using `ALTER TABLE` on at least one but not all of the underlying tables caused the table definitions to be considered different from that of the `MERGE` table, even if the `ALTER TABLE` did not change the definition. (Bug #26881)

Changes in MySQL Enterprise 5.0.36 [MRU] (2007-02-20)

This is a *Monthly Rapid Update* release of the MySQL Enterprise Server 5.0.

This section documents all changes and bug fixes that have been applied since the last MySQL Enterprise Server release (5.0.34).



Note

After release, a trigger failure problem was found to have been introduced. (Bug #27006) Users affected by this issue should upgrade to MySQL 5.0.38, which corrects the problem.

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- **Incompatible Change; MySQL Cluster:** The `LockPagesInMainMemory` configuration parameter has changed its type and possible values.



Important

The values `true` and `false` are no longer accepted for this parameter. If you were using this parameter and had it set to `false` in a previous release, you must change it to `0`. If you had this parameter set to `true`, you should instead use `1` to obtain the same behavior as previously, or `2` to take advantage of new functionality introduced with this release, as described in the section cited above.

(Bug #25686)

- **Incompatible Change:** Previously, the `DATE_FORMAT()` function returned a binary string. Now it returns a string with a character set and collation given by `character_set_connection` and `collation_connection` so that it can return month and weekday names containing non-ASCII characters. (Bug #22646)
- **Important Change:** When using a `MERGE` table, the definition of the table and the underlying `MyISAM` tables are checked each time the tables are opened for access (including any `SELECT` or `INSERT`

statement). Each table is compared for column order, types, sizes, and associated indexes. If there is a difference in any one of the tables, the statement will fail.

- The `localhost` anonymous user account created during MySQL installation on Windows now has no global privileges. Formerly this account had all global privileges. For operations that require global privileges, the `root` account can be used instead. (Bug #24496)
- The bundled yaSSL library was upgraded to version 1.5.8.

Bugs Fixed

- **Security Fix:** Using an `INFORMATION_SCHEMA` table with `ORDER BY` in a subquery could cause a server crash.

We would like to thank Oren Isacson of Flowgate Security Consulting and Stefan Streichsbier of SEC Consult for informing us of this problem. (Bug #24630, Bug #26556, CVE-2007-1420)

- **Incompatible Change:** For `ENUM` columns that had enumeration values containing commas, the commas were mapped to `0xff` internally. However, this rendered the commas indistinguishable from true `0xff` characters in the values. This no longer occurs. However, the fix requires that you dump and reload any tables that have `ENUM` columns containing any true `0xff` values. Dump the tables using `mysqldump` with the current server before upgrading from a version of MySQL 5.0 older than 5.0.36 to version 5.0.36 or newer. (Bug #24660)
- **MySQL Cluster; Partitioning:** A query with an `IN` clause against an `NDB` table employing explicit user-defined partitioning did not always return all matching rows. (Bug #25821)
- **MySQL Cluster:** It was not possible to create an `NDB` table with a key on two `VARCHAR` columns where both columns had a storage length in excess of 256. (Bug #25746)
- **MySQL Cluster:** In some circumstances, shutting down the cluster could cause connected `mysqld` processes to crash. (Bug #25668)
- **MySQL Cluster:** Memory allocations for `TEXT` columns were calculated incorrectly, resulting in space being wasted and other issues. (Bug #25562)
- **MySQL Cluster:** The failure of a master node during a node restart could lead to a resource leak, causing later node failures. (Bug #25554)
- **MySQL Cluster:** An `UPDATE` using an `IN` clause on an `NDB` table on which there was a trigger caused `mysqld` to crash. (Bug #25522)
- **MySQL Cluster:** A node shutdown occurred if the master failed during a commit. (Bug #25364)
- **MySQL Cluster:** Creating a nonunique index with the `USING HASH` clause silently created an ordered index instead of issuing a warning. (Bug #24820)
- **MySQL Cluster:** The `ndb_size.tmpl` file (necessary for using the `ndb_size.pl` script) was missing from binary distributions. (Bug #24191)
- **MySQL Cluster:** The management server did not handle logging of node shutdown events correctly in certain cases. (Bug #22013)
- **MySQL Cluster:** `SELECT` statements with a `BLOB` or `TEXT` column in the selected column list and a `WHERE` condition including a primary key lookup on a `VARCHAR` primary key produced empty result sets. (Bug #19956)
- **MySQL Cluster:** The loss of one or more data nodes could sometimes cause `ndb_mgmd` to use a high amount of CPU (15 percent or more, as opposed to 1 to 2 percent normally).

- **Replication:** When `SET PASSWORD` was written to the binary log, double quotation marks were included in the statement. If the slave was running in with the server SQL mode set to `ANSI_QUOTES`, then the event failed, which halted the replication process. (Bug #24158)
- **Replication:** A stored procedure, executed from a connection using a binary character set, and which wrote multibyte data, would write incorrectly escaped entries to the binary log. This caused syntax errors, and caused replication to fail. (Bug #23619, Bug #24492)
- **Replication:** Changes to the `lc_time_names` system variable were not replicated. (Bug #22645)
- **Replication:** For `SET`, `SELECT`, and `DO` statements that invoked a stored function from a database other than the default database, the function invocation could fail to be replicated. (Bug #19725)
- **Replication:** If a slave server closed its relay log (for example, due to an error during log rotation), the I/O thread did not recognize this and still tried to write to the log, causing a server crash. (Bug #10798)
- **Cluster API:** Deletion of an `Ndb_cluster_connection` object took a very long time. (Bug #25487)
- **Cluster API:** `libndbclient.so` was not versioned. (Bug #13522)
- Using `ORDER BY` or `GROUP BY` could yield different results when selecting from a view and selecting from the underlying table. (Bug #26209)
- `DISTINCT` queries that were executed using a loose scan for an `InnoDB` table that had been emptied caused a server crash. (Bug #26159)
- A `WHERE` clause that used `BETWEEN` for `DATETIME` values could be treated differently for a `SELECT` and a view defined as that `SELECT`. (Bug #26124)
- Collation for `LEFT JOIN` comparisons could be evaluated incorrectly, leading to improper query results. (Bug #26017)
- The `WITH CHECK OPTION` clause for views was ignored for updates of multiple-table views when the updates could not be performed on fly and the rows to update had to be put into temporary tables first. (Bug #25931)
- `LOAD DATA INFILE` did not work with pipes. (Bug #25807)
- The `SEC_TO_TIME()` and `QUARTER()` functions sometimes did not handle `NULL` values correctly. (Bug #25643)
- The `InnoDB` parser sometimes did not account for null bytes, causing spurious failure of some queries. (Bug #25596)
- View definitions that used the `!` operator were treated as containing the `NOT` operator, which has a different precedence and can produce different results. . (Bug #25580)
- An error in the name resolution of nested `JOIN ... USING` constructs was corrected. (Bug #25575)
- `GROUP BY` and `DISTINCT` did not group `NULL` values for columns that have a `UNIQUE` index. . (Bug #25551)
- The `--with-readline` option for `configure` did not work for commercial source packages, but no error message was printed to that effect. Now a message is printed. (Bug #25530)
- A yaSSL program named `test` was installed, causing conflicts with the `test` system utility. It is no longer installed. (Bug #25417)
- For a `UNIQUE` index containing many `NULL` values, the optimizer would prefer the index for `col IS NULL` conditions over other more selective indexes. . (Bug #25407)

- An `AFTER UPDATE` trigger on an `InnoDB` table with a composite primary key caused the server to crash. (Bug #25398)
- Passing a `NULL` value to a user-defined function from within a stored procedure crashes the server. (Bug #25382)
- `pererror` crashed on some platforms due to failure to handle a `NULL` pointer. (Bug #25344)
- `mysql.server stop` timed out too quickly (35 seconds) waiting for the server to exit. Now it waits up to 15 minutes, to ensure that the server exits. (Bug #25341)
- A query that contained an `EXIST` subquery with a `UNION` over correlated and uncorrelated `SELECT` queries could cause the server to crash. (Bug #25219)
- `mysql_kill()` caused a server crash when used on an SSL connection. (Bug #25203)
- `yaSSL` was sensitive to the presence of whitespace at the ends of lines in PEM-encoded certificates, causing a server crash. (Bug #25189)
- A query with `ORDER BY` and `GROUP BY` clauses where the `ORDER BY` clause had more elements than the `GROUP BY` clause caused a memory overrun leading to a crash of the server. (Bug #25172)
- Use of `ON DUPLICATE KEY UPDATE` defeated the usual restriction against inserting into a join-based view unless only one of the underlying tables is used. (Bug #25123)
- `ALTER TABLE ... ENABLE KEYS` acquired a global lock, preventing concurrent execution of other statements that use tables. . (Bug #25044)
- A return value of `-1` from user-defined handlers was not handled well and could result in conflicts with server code. (Bug #24987)
- Accessing a fixed record format table with a crashed key definition results in server/`myisamchk` segmentation fault. (Bug #24855)
- `mysqld_multi` and `mysqlaccess` looked for option files in `/etc` even if the `--sysconfdir` option for `configure` had been given to specify a different directory. (Bug #24780)
- If there was insufficient memory available to `mysqld`, this could sometimes cause the server to hang during startup. (Bug #24751)
- If an `ORDER BY` or `GROUP BY` list included a constant expression being optimized away and, at the same time, containing single-row subselects that returned more than one row, no error was reported. If a query required sorting by expressions containing single-row subselects that returned more than one row, execution of the query could cause a server crash. (Bug #24653)
- For `ALTER TABLE`, using `ORDER BY expression` could cause a server crash. Now the `ORDER BY` clause permits only column names to be specified as sort criteria (which was the only documented syntax, anyway). (Bug #24562)
- A workaround was implemented to avoid a race condition in the NPTL `pthread_exit()` implementation. (Bug #24507)
- `mysqltest` crashed with a stack overflow. (Bug #24498)
- Within stored routines or prepared statements, inconsistent results occurred with multiple use of `INSERT ... SELECT ... ON DUPLICATE KEY UPDATE` when the `ON DUPLICATE KEY UPDATE` clause erroneously tried to assign a value to a column mentioned only in its `SELECT` part. (Bug #24491)

- Expressions of the form `(a, b) IN (SELECT a, MIN(b) FROM t GROUP BY a)` could produce incorrect results when column `a` of table `t` contained `NULL` values while column `b` did not. (Bug #24420)
- If a prepared statement accessed a view, access to the tables listed in the query after that view was checked in the security context of the view. (Bug #24404)
- Attempts to access a `MyISAM` table with a corrupt column definition caused a server crash. (Bug #24401)
- When opening a corrupted `.frm` file during a query, the server crashes. (Bug #24358)
- A query using `WHERE unsigned_column NOT IN ('negative_value')` could cause the server to crash. (Bug #24261)
- Expressions of the form `(a, b) IN (SELECT c, d ...)` could produce incorrect results if `a`, `b`, or both were `NULL`. (Bug #24127)
- A `FETCH` statement using a cursor on a table which was not in the table cache could sometimes cause the server to crash. (Bug #24117)
- Queries that evaluate `NULL IN (SELECT ... UNION SELECT ...)` could produce an incorrect result (`FALSE` instead of `NULL`). (Bug #24085)
- Hebrew-to-Unicode conversion failed for some characters. Definitions for the following Hebrew characters (as specified by the ISO/IEC 8859-8:1999) were added: LEFT-TO-RIGHT MARK (LRM), RIGHT-TO-LEFT MARK (RLM) (Bug #24037)
- Some `UPDATE` statements were slower than in previous versions when the search key could not be converted to a valid value for the type of the search column. (Bug #24035)
- `ISNULL(DATE(NULL))` and `ISNULL(CAST(NULL AS DATE))` erroneously returned false. (Bug #23938)
- Within a stored routine, accessing a declared routine variable with `PROCEDURE ANALYSE()` caused a server crash. (Bug #23782)
- When reading from the standard input on Windows, `mysqlbinlog` opened the input in text mode rather than binary mode and consequently misinterpreted some characters such as **Control+Z**. (Bug #23735)
- For an `InnoDB` table with any `ON DELETE` trigger, `TRUNCATE TABLE` mapped to `DELETE` and activated triggers. Now a fast truncation occurs and triggers are not activated. . (Bug #23556)
- The row count for `MyISAM` tables was not updated properly, causing `SHOW TABLE STATUS` to report incorrect values. (Bug #23526)
- With `ONLY_FULL_GROUP_BY` enabled, the server was too strict: Some expressions involving only aggregate values were rejected as nonaggregate (for example, `MAX(a) - MIN(a)`). (Bug #23417)
- The arguments to the `ENCODE()` and the `DECODE()` functions were not printed correctly, causing problems in the output of `EXPLAIN EXTENDED` and in view definitions. (Bug #23409)
- Some queries against `INFORMATION_SCHEMA` that used subqueries failed. . (Bug #23299)
- `readline` detection did not work correctly on NetBSD. (Bug #23293)
- If there was insufficient memory to store or update a blob record in a `MyISAM` table then the table will be marked as crashed. (Bug #23196)
- `LAST_INSERT_ID()` was not reset to 0 if `INSERT ... SELECT` inserted no rows. (Bug #23170)

- The number of `setsockopt()` calls performed for reads and writes to the network socket was reduced to decrease system call overhead. (Bug #22943)
- `mysql_upgrade` failed when called with a `--basedir` path name containing spaces. (Bug #22801)
- `SET lc_time_names = value` permitted only exact literal values, not expression values. (Bug #22647)
- The `STDDEV()` function returned a positive value for data sets consisting of a single value. (Bug #22555)
- Storing values specified as hexadecimal values 64 or more bits long in `BIT(64)`, `BIGINT`, or `BIGINT UNSIGNED` columns did not raise any warning or error if the value was out of range. (Bug #22533)
- `SHOW COLUMNS` reported some `NOT NULL` columns as `NULL`. (Bug #22377)
- Type conversion errors during formation of index search conditions were not correctly checked, leading to incorrect query results. (Bug #22344)
- The code for generating `USE` statements for binary logging of `CREATE PROCEDURE` statements resulted in confusing output from `mysqlbinlog` for `DROP PROCEDURE` statements. (Bug #22043)
- For the `IF()` and `COALESCE()` function and `CASE` expressions, large unsigned integer values could be mishandled and result in warnings. (Bug #22026)
- SSL connections could hang at connection shutdown. (Bug #21781, Bug #24148)
- When updating a table that used a `JOIN` of the table itself (for example, when building trees) and the table was modified on one side of the expression, the table would either be reported as crashed or the wrong rows in the table would be updated. (Bug #21310)
- Inserting `DEFAULT` into a column with no default value could result in garbage in the column. Now the same result occurs as when inserting `NULL` into a `NOT NULL` column. (Bug #20691)
- A stored routine containing semicolon in its body could not be reloaded from a dump of a binary log. (Bug #20396)
- `SELECT ... FOR UPDATE`, `SELECT ... LOCK IN SHARE MODE`, `DELETE`, and `UPDATE` statements executed using a full table scan were not releasing locks on rows that did not satisfy the `WHERE` condition. (Bug #20390)
- On Windows, if the server was installed as a service, it did not auto-detect the location of the data directory. (Bug #20376)
- The `BUILD/check-cpu` script did not recognize Celeron processors. (Bug #20061)
- If a duplicate key value was present in the table, `INSERT ... ON DUPLICATE KEY UPDATE` reported a row count indicating that a record was updated, even when no record actually changed due to the old and new values being the same. Now it reports a row count of zero. (Bug #19978)

References: See also: Bug #27006, Bug #27033, Bug #27210.

- `ORDER BY` values of the `DOUBLE` or `DECIMAL` types could change the result returned by a query. (Bug #19690)
- The `readline` library wrote to uninitialized memory, causing `mysql` to crash. (Bug #19474)
- `mysqltest` incorrectly tried to retrieve result sets for some queries where no result set was available. (Bug #19410)
- Use of already freed memory caused SSL connections to hang forever. (Bug #19209)

- The server might fail to use an appropriate index for `DELETE` when `ORDER BY`, `LIMIT`, and a nonrestricting `WHERE` are present. (Bug #17711)
- No warning was issued for use of the `DATA DIRECTORY` or `INDEX DIRECTORY` table options on a platform that does not support them. (Bug #17498)
- When a prepared statement failed during the prepare operation, the error code was not cleared when it was reused, even if the subsequent use was successful. (Bug #15518)
- On Windows, the `SLEEP()` function could sleep too long, especially after a change to the system clock. (Bug #14094, Bug #24686, Bug #17635)
- `mysqldump --order-by-primary` failed if the primary key name was an identifier that required quoting. (Bug #13926)
- To enable installation of MySQL RPMs on Linux systems running RHEL 4 (which includes SE-Linux) additional information was provided to specify some actions that are permitted to the MySQL binaries. (Bug #12676)
- The presence of `ORDER BY` in a view definition prevented the `MERGE` algorithm from being used to resolve the view even if nothing else in the definition required the `TEMPTABLE` algorithm. (Bug #12122)

Changes in MySQL Enterprise 5.0.34 [MRU] (2007-01-17)

This is a *Monthly Rapid Update* release of the MySQL Enterprise Server 5.0.

This section documents all changes and bug fixes that have been applied since the last MySQL Enterprise Server release (5.0.32).

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- The `--skip-thread-priority` option now is enabled by default for binary Mac OS X distributions. Use of thread priorities degrades performance on Mac OS X. (Bug #18526)
- Added the `--disable-grant-options` option to `configure`. If `configure` is run with this option, the `--bootstrap`, `--skip-grant-tables`, and `--init-file` options for `mysqld` are disabled and cannot be used. For Windows, the `configure.js` script recognizes the `DISABLE_GRANT_OPTIONS` flag, which has the same effect.

Bugs Fixed

- **MySQL Cluster:** Hosts in clusters with large numbers of nodes could experience excessive CPU usage while obtaining configuration data. (Bug #25711)
- **MySQL Cluster:** When a data node was shut down using the management client `STOP` command, a connection event (`NDB_LE_Connected`) was logged instead of a disconnection event (`NDB_LE_Disconnected`). (Bug #22773)
- **Cluster API:** Invoking the `NdbTransaction::execute()` method using execution type `Commit` and abort option `AO_IgnoreError` could lead to a crash of the transaction coordinator (`DBTC`). (Bug #25090)
- **Cluster API:** A unique index lookup on a nonexistent tuple could lead to a data node timeout (error 4012). (Bug #25059)

- Referencing an ambiguous column alias in an expression in the `ORDER BY` clause of a query caused the server to crash. (Bug #25427)
- Using a view in combination with a `USING` clause caused column aliases to be ignored. (Bug #25106)
- A multiple-table `DELETE QUICK` could sometimes cause one of the affected tables to become corrupted. (Bug #25048)
- An assertion failed incorrectly for prepared statements that contained a single-row uncorrelated subquery that was used as an argument of the `IS NULL` predicate. (Bug #25027)
- Optimizations that are legal only for subqueries without tables and `WHERE` conditions were applied for any subquery without tables. (Bug #24670)
- Some joins in which one of the joined tables was a view could return erroneous results or crash the server. (Bug #24345)
- A view was not handled correctly if the `SELECT` part contained “\z”. (Bug #24293)
- The server was built even when `configure` was run with the `--without-server` option. (Bug #23973)

References: See also: Bug #32898.

- `OPTIMIZE TABLE` tried to sort R-tree indexes such as spatial indexes, although this is not possible (see [OPTIMIZE TABLE Syntax](#)). (Bug #23578)
- User-defined variables could consume excess memory, leading to a crash caused by the exhaustion of resources available to the `MEMORY` storage engine, due to the fact that this engine is used by MySQL for variable storage and intermediate results of `GROUP BY` queries. Where `SET` had been used, such a condition could instead give rise to the misleading error message `You may only use constant expressions with SET`, rather than `Out of memory (Needed NNNNNN bytes)`. (Bug #23443)
- A table created with the `ROW_FORMAT = FIXED` table option lost that option if an index was added or dropped with `CREATE INDEX` or `DROP INDEX`. (Bug #23404)
- A deadlock could occur, with the server hanging on `Closing tables`, with a sufficient number of concurrent `INSERT DELAYED`, `FLUSH TABLES`, and `ALTER TABLE` operations. (Bug #23312)
- A compressed `MyISAM` table that became corrupted could crash `myisamchk` and possibly the MySQL Server. (Bug #23139)
- Changing the value of `MI_KEY_BLOCK_LENGTH` in `myisam.h` and recompiling MySQL resulted in a `myisamchk` that saw existing `MyISAM` tables as corrupt. (Bug #22119)
- A crash of the MySQL Server could occur when unpacking a `BLOB` column from a row in a corrupted `MyISAM` table. This could happen when trying to repair a table using either `REPAIR TABLE` or `myisamchk`; it could also happen when trying to access such a “broken” row using statements like `SELECT` if the table was not marked as crashed. (Bug #22053)
- The `FEDERATED` storage engine did not support the `euckr` character set. (Bug #21556)
- `mysqld_error.h` was not installed when only the client libraries were built. (Bug #21265)
- `InnoDB`: During a restart of the MySQL Server that followed the creation of a temporary table using the `InnoDB` storage engine, MySQL failed to clean up in such a way that `InnoDB` still attempted to find the files associated with such tables. (Bug #20867)

- **InnoDB:** Optimizations removed in MySQL 5.0.28 were re-enabled except for files under the `innobase/mem` directory. (This is a fine-tuning of optimization disabling.) (Bug #19424)
- Some **CASE** statements inside stored routines could lead to excessive resource usage or a crash of the server. (Bug #19194, Bug #24854)
- Instance Manager could crash during shutdown. (Bug #19044)
- The **FEDERATED** storage engine did not support the `utf8` character set. (Bug #17044)
- The optimizer removes expressions from **GROUP BY** and **DISTINCT** clauses if they happen to participate in `expression = constant` predicates of the **WHERE** clause, the idea being that, if the expression is equal to a constant, then it cannot take on multiple values. However, for predicates where the expression and the constant item are of different result types (for example, when a string column is compared to 0), this is not valid, and can lead to invalid results in such cases. The optimizer now performs an additional check of the result types of the expression and the constant; if their types differ, then the expression is not removed from the **GROUP BY** list. (Bug #15881)
- Dropping a user-defined function sometimes did not remove the UDF entry from the `mysql.proc` table. (Bug #15439)
- Inserting a row into a table without specifying a value for a **BINARY(N) NOT NULL** column caused the column to be set to spaces, not zeros. (Bug #14171)

Changes in MySQL Community Server 5.0.33 (2007-01-09)

This is a bugfix release for the current MySQL Community Server production release family. It replaces MySQL 5.0.27.



Note

This version of MySQL Community Server has been released as a source tarball only; there are no binaries built by MySQL.

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- **Incompatible Change:** **InnoDB** rolls back only the last statement on a transaction timeout. A new option, `--innodb_rollback_on_timeout`, causes **InnoDB** to abort and roll back the entire transaction if a transaction timeout occurs (the same behavior as in MySQL 5.0.13 and earlier). (Bug #24200)
- **Incompatible Change:** The `prepared_stmt_count` system variable has been converted to the `Prepared_stmt_count` global status variable (viewable with the `SHOW GLOBAL STATUS` statement). (Bug #23159)
- **MySQL Cluster:** Setting the configuration parameter `LockPagesInMainMemory` had no effect. (Bug #24461)
- **MySQL Cluster:** The `ndb_config` utility now accepts `-c` as a short form of the `--ndb-connectstring` option. (Bug #22295)
- **MySQL Cluster:** Added the `--bind-address` option for `ndbd`. This permits a data node process to be bound to a specific network interface. (Bug #22195)

- **MySQL Cluster:** It is now possible to create a unique hashed index on a column that is not defined as `NOT NULL`.



Note

This change applies only to tables using the `NDB` storage engine.

Unique indexes on columns in `NDB` tables do not store null values because they are mapped to primary keys in an internal index table (and primary keys cannot contain nulls).

Normally, an additional ordered index is created when one creates unique indexes on `NDB` table columns; this can be used to search for `NULL` values. However, if `USING HASH` is specified when such an index is created, no ordered index is created.

The reason for permitting unique hash indexes with null values is that, in some cases, the user wants to save space if a large number of records are pre-allocated but not fully initialized. This also assumes that the user will *not* try to search for null values. Since MySQL does not support indexes that are not permitted to be searched in some cases, the `NDB` storage engine uses a full table scan with pushed conditions for the referenced index columns to return the correct result.

A warning is returned if one creates a unique nullable hash index, since the query optimizer should be provided a hint not to use it with `NULL` values if this can be avoided. (Bug #21507)

- **MySQL Cluster:** The `Ndb_number_of_storage_nodes` system variable was renamed to `Ndb_number_of_data_nodes`. (Bug #20848)
- **MySQL Cluster:** The `HELP` command in the Cluster management client now provides command-specific help. For example, `HELP RESTART` in `ndb_mgm` provides detailed information about the `RESTART` command. (Bug #19620)
- `DROP TRIGGER` now supports an `IF EXISTS` clause. (Bug #23703)
- The `Com_create_user` status variable was added (for counting `CREATE USER` statements). (Bug #22958)
- The `--memlock` option relies on system calls that are unreliable on some operating systems. If a crash occurs, the server now checks whether `--memlock` was specified and if so issues some information about possible workarounds. (Bug #22860)
- If the user specified the server options `--max-connections=N` or `--table-cache=M`, a warning would be given in some cases that some values were recalculated, with the result that `--table-cache` could be assigned greater value.

In such cases, both the warning and the increase in the `--table-cache` value were completely harmless. Note also that it is not possible for the MySQL Server to predict or to control limitations on the maximum number of open files, since this is determined by the operating system.

The value of `--table-cache` is no longer increased automatically, and a warning is now given only if some values had to be decreased due to operating system limits. (Bug #21915)

- For the `CALL` statement, stored procedures that take no arguments now can be invoked without parentheses. That is, `CALL p()` and `CALL p` are equivalent. (Bug #21462)
- `mysql_upgrade` now passes all the parameters specified on the command line to both `mysqlcheck` and `mysql` using the `upgrade_defaults` file. (Bug #20100)
- `SHOW STATUS` is no longer logged to the slow query log. (Bug #19764)

- `mysqldump --single-transaction` now uses `START TRANSACTION /*!40100 WITH CONSISTENT SNAPSHOT */` rather than `BEGIN` to start a transaction, so that a consistent snapshot will be used on those servers that support it. (Bug #19660)
- The bundled yaSSL library was upgraded to version 1.5.0.

Bugs Fixed

- **Performance:** The `InnoDB` mutex structure was simplified to reduce memory load. (Bug #24386)
- **Performance:** `InnoDB` exhibited thread thrashing with more than 50 concurrent connections under an update-intensive workload. (Bug #22868)
- **Performance:** Evaluation of subqueries that require the filesort algorithm were allocating and freeing the `sort_buffer_size` buffer many times, resulting in slow performance. Now the buffer is allocated once and reused. (Bug #21727)
- **Performance:** `InnoDB` showed substandard performance with multiple queries running concurrently. (Bug #15815)
- **MySQL Cluster:** The failure of a data node failure during a schema operation could lead to additional node failures. (Bug #24752)
- **MySQL Cluster:** A committed read could be attempted before a data node had time to connect, causing a timeout error. (Bug #24717)
- **MySQL Cluster:** Sudden disconnection of an SQL or data node could lead to shutdown of data nodes with the error `failed ndbrequire`. (Bug #24447)
- **MySQL Cluster:** `ndb_config` failed when trying to use 2 management servers and node IDs. (Bug #23887)
- **MySQL Cluster:** Backup of a cluster failed if there were any tables with 128 or more columns. (Bug #23502)
- **MySQL Cluster:** Cluster backups failed when there were more than 2048 schema objects in the cluster. (Bug #23499)
- **MySQL Cluster:** The management client command `ALL DUMP 1000` would cause the cluster to crash if data nodes were connected to the cluster but not yet fully started. (Bug #23203)
- **MySQL Cluster:** `INSERT ... ON DUPLICATE KEY UPDATE` on an `NDB` table could lead to deadlocks and memory leaks. (Bug #23200)
- **MySQL Cluster:** (NDB API): Inactivity timeouts for scans were not correctly handled. (Bug #23107)
- **MySQL Cluster:** If a node restart could not be performed from the REDO log, no node takeover took place. This could cause partitions to be left empty during a system restart. (Bug #22893)
- **MySQL Cluster:** Multiple node restarts in rapid succession could cause a system restart to fail , or induce a race condition. (Bug #22892, Bug #23210)
- **MySQL Cluster:** (NDB API): Attempting to read a nonexistent tuple using `Commit` mode for `NdbTransaction::execute()` caused node failures. (Bug #22672)
- **MySQL Cluster:** The `--help` output from `NDB` binaries did not include file-related options. (Bug #21994)
- **MySQL Cluster:** (NDB API): Scans closed before being executed were still placed in the send queue. (Bug #21941)

- **MySQL Cluster:** A scan timeout returned Error 4028 (`Node failure caused abort of transaction`) instead of Error 4008 (`Node failure caused abort of transaction...`). (Bug #21799)
- **MySQL Cluster:** The node recovery algorithm was missing a version check for tables in the `ALTER_TABLE_COMMITTED` state (as opposed to the `TABLE_ADD_COMMITTED` state, which has the version check). This could cause inconsistent schemas across nodes following node recovery. (Bug #21756)
- **MySQL Cluster:** The output for the `--help` option used with NDB executable programs (such as `ndbd`, `ndb_mgm`, `ndb_restore`, `ndb_config`, and others mentioned in [MySQL Cluster Programs](#)) referred to the `Ndb.cfg` file, instead of to `my.cnf`. (Bug #21585)
- **MySQL Cluster:** Partition distribution keys were updated only for the primary and starting replicas during node recovery. This could lead to node failure recovery for clusters having an odd number of replicas.

**Note**

For best results, use values for `NumberOfReplicas` that are even powers of 2.

(Bug #21535)

- **MySQL Cluster:** The `ndb_mgm` management client did not set the exit status on errors, always returning 0 instead. (Bug #21530)
- **MySQL Cluster:** Cluster logs were not rotated following the first rotation cycle. (Bug #21345)
- **MySQL Cluster:** When inserting a row into an NDB table with a duplicate value for a nonprimary unique key, the error issued would reference the wrong key. (Bug #21072)
- **MySQL Cluster:** Condition pushdown did not work correctly with `DATETIME` columns. (Bug #21056)
- **MySQL Cluster:** Under some circumstances, local checkpointing would hang, keeping any unstarted nodes from being started. (Bug #20895)
- **MySQL Cluster:** Using an invalid node ID with the management client `STOP` command could cause `ndb_mgm` to hang. (Bug #20575)
- **MySQL Cluster:** Data nodes added while the cluster was running in single user mode were all assigned node ID 0, which could later cause multiple node failures. Adding nodes while in single user mode is no longer possible. (Bug #20395)
- **MySQL Cluster:** In some cases where `SELECT COUNT(*)` from an NDB table should have yielded an error, `MAX_INT` was returned instead. (Bug #19914)
- **MySQL Cluster:** Following the restart of a management node, the Cluster management client did not automatically reconnect. (Bug #19873)
- **MySQL Cluster:** Error messages given when trying to make online changes to parameters such as `NoOfReplicas` that can only be changed using a complete shutdown and restart of the cluster did not indicate the true nature of the problem. (Bug #19787)
- **MySQL Cluster:** `ndb_restore` did not always make clear that it had recovered successfully from temporary errors while restoring a cluster backup. (Bug #19651)
- **MySQL Cluster:** In rare situations with resource shortages, a crash could result from an insufficient number of `IndexScanOperation` objects. (Bug #19198)

- **MySQL Cluster:** `ndb_mgm -e show | head` would hang after displaying the first 10 lines of output. (Bug #19047)
- **MySQL Cluster:** The error returned by the cluster when too many nodes were defined did not make clear the nature of the problem. (Bug #19045)
- **MySQL Cluster:** A unique constraint violation was not ignored by an `UPDATE IGNORE` statement when the constraint violation occurred on a nonprimary key. (Bug #18487, Bug #24303)
- **MySQL Cluster:** The `ndb_config` utility did not perform host lookups correctly when using the `--host` option (Bug #17582)
- **MySQL Cluster:** A problem with takeover during a system restart caused ordered indexes to be rebuilt incorrectly. (Bug #15303)
- **Replication:** Changes to character set variables prior to an action on a replication-ignored table were forgotten by slave servers. (Bug #22877)
- **Replication:** On slave servers, transactions that exceeded the lock wait timeout failed to roll back properly. (Bug #20697)
- **Replication:** Column names were not quoted properly for replicated views. (Bug #19736)
- **Replication:** SQL statements close to the size of `max_allowed_packet` could produce binary log events larger than `max_allowed_packet` that could not be read by slave servers. (Bug #19402)
- **Replication:** Slave servers would retry the execution of an SQL statement an infinite number of times, ignoring the value `SLAVE_TRANSACTION_RETRIES` when using the NDB engine. (Bug #16228)
- **Replication:** Transient errors in replication from master to slave may trigger multiple `Got fatal error 1236: 'binlog truncated in the middle of event'` errors on the slave. (Bug #4053)
- **Cluster API:** Using `BIT` values with any of the comparison methods of the `NdbScanFilter` class caused data nodes to fail. (Bug #24503)
- **Cluster API:** Some MGM API function calls could yield incorrect return values in certain cases where the cluster was operating under a very high load, or experienced timeouts in inter-node communications. (Bug #24011)
- **Cluster API:** The `NdbOperation::getBlobHandle()` method, when called with the name of a nonexistent column, caused a segmentation fault. (Bug #21036)
- **Cluster API:** When multiple processes or threads in parallel performed the same ordered scan with exclusive lock and updated the retrieved records, the scan could skip some records, which as a result were not updated. (Bug #20446)
- The `REPEAT()` function could return `NULL` when passed a column for the count argument. (Bug #24947)
- `mysql_upgrade` failed if the `--password` (or `-p`) option was given. (Bug #24896)
- With `innodb_file_per_table` enabled, InnoDB displayed incorrect file times in the output from `SHOW TABLE STATUS`. (Bug #24712)
- `ALTER TABLE ENABLE KEYS` or `ALTER TABLE DISABLE KEYS` combined with another `ALTER TABLE` option other than `RENAME TO` did nothing. In addition, if `ALTER TABLE` was used on a table having disabled keys, the keys of the resulting table were enabled. (Bug #24395)
- The `--extern` option for `mysql-test-run.pl` did not function correctly. (Bug #24354)

- Foreign key identifiers for `InnoDB` tables could not contain certain characters. (Bug #24299)
- The `mysql.server` script used the `source` command, which is less portable than the `.` command; it now uses `.` instead. (Bug #24294)
- `ALTER TABLE` statements that performed both `RENAME TO` and `{ENABLE|DISABLE} KEYS` operations caused a server crash. (Bug #24219)
- The loose index scan optimization for `GROUP BY` with `MIN` or `MAX` was not applied within other queries, such as `CREATE TABLE ... SELECT ...`, `INSERT ... SELECT ...`, or in the `FROM` clauses of subqueries. (Bug #24156)
- There was a race condition in the `InnoDB fil_flush_file_spaces()` function. (Bug #24089)

References: This issue is a regression of: Bug #15653.

- Subqueries for which a pushed-down condition did not produce exactly one key field could cause a server crash. (Bug #24056)
- The size of `MEMORY` tables and internal temporary tables was limited to 4GB on 64-bit Windows systems. (Bug #24052)
- yaSSL-related memory leaks were detected by Valgrind. (Bug #23981)
- The internal SQL interpreter of `InnoDB` placed an unnecessary lock on the supremum record with `innodb_locks_unsafe_for_binlog` enabled. This caused an assertion failure when `InnoDB` was built with debugging enabled. (Bug #23769)
- `ROW_COUNT()` did not work properly as an argument to a stored procedure. (Bug #23760)
- `LAST_DAY('0000-00-00')` could cause a server crash. (Bug #23653)
- A trigger that invoked a stored function could cause a server crash when activated by different client connections. (Bug #23651)
- The stack size for NetWare binaries was increased to 128KB to prevent problems caused by insufficient stack size. (Bug #23504)
- If elements in a nontop-level `IN` subquery were accessed by an index and the subquery result set included a `NULL` value, the quantified predicate that contained the subquery was evaluated to `NULL` when it should return a non-`NULL` value. (Bug #23478)
- When applying the `group_concat_max_len` limit, `GROUP_CONCAT()` could truncate multibyte characters in the middle. (Bug #23451)
- MySQL 5.0.26 introduced an ABI incompatibility, which this release reverts. Programs compiled against 5.0.26 are not compatible with any other version and must be recompiled. (Bug #23427)
- `M % 0` returns `NULL`, but `(M % 0) IS NULL` evaluated to false. (Bug #23411)
- `mysql_affected_rows()` could return values different from `mysql_stmt_affected_rows()` for the same sequence of statements. (Bug #23383)
- For not-yet-authenticated connections, the `Time` column in `SHOW PROCESSLIST` was a random value rather than `NULL`. (Bug #23379)
- Accuracy was improved for comparisons between `DECIMAL` columns and numbers represented as strings. (Bug #23260)
- MySQL failed to build on Linux/Alpha. (Bug #23256)

References: This issue is a regression of: Bug #21250.

- If `COMPRESS()` returned `NULL`, subsequent invocations of `COMPRESS()` within a result set or within a trigger also returned `NULL`. (Bug #23254)
- Calculation of `COUNT(DISTINCT)`, `AVG(DISTINCT)`, or `SUM(DISTINCT)` when they are referenced more than once in a single query with `GROUP BY` could cause a server crash. (Bug #23184)
- Insufficient memory (`myisam_sort_buffer_size`) could cause a server crash for several operations on `MyISAM` tables: repair table, create index by sort, repair by sort, parallel repair, bulk insert. (Bug #23175)
- The column default value in the output from `SHOW COLUMNS` or `SELECT FROM INFORMATION_SCHEMA.COLUMNS` was truncated to 64 characters. (Bug #23037)
- `mysql` did not check for errors when fetching data during result set printing. (Bug #22913)
- The return value from `my_seek()` was ignored. (Bug #22828)
- The optimizer failed to use equality propagation for `BETWEEN` and `IN` predicates with string arguments. (Bug #22753)
- The `Handler_rollback` status variable sometimes was incremented when no rollback had taken place. (Bug #22728)
- The `Host` column in `SHOW PROCESSLIST` output was blank when the server was started with the `--skip-grant-tables` option. (Bug #22723)
- If a table contains an `AUTO_INCREMENT` column, inserting into an insertable view on the table that does not include the `AUTO_INCREMENT` column should not change the value of `LAST_INSERT_ID()`, because the side effects of inserting default values into columns not part of the view should not be visible. MySQL was incorrectly setting `LAST_INSERT_ID()` to zero. (Bug #22584)
- Queries using a column alias in an expression as part of an `ORDER BY` clause failed, an example of such a query being `SELECT mycol + 1 AS mynum FROM mytable ORDER BY 30 - mynum`. (Bug #22457)
- Using `EXPLAIN` caused a server crash for queries that selected from `INFORMATION_SCHEMA` in a subquery in the `FROM` clause. (Bug #22413)
- Instance Manager had a race condition involving `mysqld` PID file removal. (Bug #22379)
- A server crash occurred when using `LOAD DATA` to load a table containing a `NOT NULL` spatial column, when the statement did not load the spatial column. Now a `NULL supplied to NOT NULL column` error occurs. (Bug #22372)
- The optimizer used the `ref` join type rather than `eq_ref` for a simple join on strings. (Bug #22367)
- Some queries that used `MAX()` and `GROUP BY` could incorrectly return an empty result. (Bug #22342)
- `DATE_ADD()` requires complete dates with no “zero” parts, but sometimes did not return `NULL` when given such a date. (Bug #22229)
- If an `init_connect` SQL statement produced an error, the connection was silently terminated with no error message. Now the server writes a warning to the error log. (Bug #22158)
- Some small double precision numbers (such as `1.00000001e-300`) that should have been accepted were truncated to zero. (Bug #22129)

- For a nonexistent table, `DROP TEMPORARY TABLE` failed with an incorrect error message if `read_only` was enabled. (Bug #22077)
- Trailing spaces were not removed from Unicode `CHAR` column values when used in indexes. This resulted in excessive usage of storage space, and could affect the results of some `ORDER BY` queries that made use of such indexes.

**Note**

When upgrading, it is necessary to re-create any existing indexes on Unicode `CHAR` columns of each affected table to take advantage of the fix. See [Rebuilding or Repairing Tables or Indexes](#).

(Bug #22052)

- The code for generating `USE` statements for binary logging of `CREATE PROCEDURE` statements resulted in confusing output from `mysqlbinlog` for `DROP PROCEDURE` statements. (Bug #22043)
- `STR_TO_DATE()` returned `NULL` if the format string contained a space following a nonformat character. (Bug #22029)
- Use of a DES-encrypted SSL certificate file caused a server crash. (Bug #21868)
- Use of `PREPARE` with a `CREATE PROCEDURE` statement that contained a syntax error caused a server crash. (Bug #21856)
- Adding a day, month, or year interval to a `DATE` value produced a `DATE`, but adding a week interval produced a `DATETIME` value. Now all produce a `DATE` value. (Bug #21811)
- In some cases, the parser failed to distinguish a user-defined function from a stored function. (Bug #21809)
- Use of a subquery that invoked a function in the column list of the outer query resulted in a memory leak. (Bug #21798)
- Inserting a default or invalid value into a spatial column could fail with `Unknown error` rather than a more appropriate error. (Bug #21790)
- It was possible to use `DATETIME` values whose year, month, and day parts were all zeros but whose hour, minute, and second parts contained nonzero values, an example of such an illegal `DATETIME` being `'0000-00-00 11:23:45'`.

**Note**

This fix was reverted in MySQL 5.0.40.

(Bug #21789)

References: See also: Bug #25301.

- yaSSL crashed on pre-Pentium Intel CPUs. (Bug #21765)
- Through the C API, the member strings in `MYSQL_FIELD` for a query that contained expressions could return incorrect results. (Bug #21635)
- Selecting from a `MERGE` table could result in a server crash if the underlying tables had fewer indexes than the `MERGE` table itself. (Bug #21617, Bug #22937)

- View columns were always handled as having implicit derivation, leading to `illegal mix of collation errors` for some views in `UNION` operations. Now view column derivation comes from the original expression given in the view definition. (Bug #21505)
- `InnoDB` crashed while performing XA recovery of prepared transactions. (Bug #21468)
- `INET_ATON()` returned a signed `BIGINT` value, not an unsigned value. (Bug #21466)
- After `FLUSH TABLES WITH READ LOCK` followed by `UNLOCK TABLES`, attempts to drop or alter a stored routine failed with an error that the routine did not exist, and attempts to execute the routine failed with a lock conflict error. (Bug #21414)
- It was possible to set the backslash character (“\”) as the delimiter character using `DELIMITER`, but not actually possible to use it as the delimiter. (Bug #21412)
- For multiple-table `UPDATE` statements, storage engines were not notified of duplicate-key errors. (Bug #21381)
- Within a prepared statement, `SELECT (COUNT(*) = 1)` (or similar use of other aggregate functions) did not return the correct result for statement re-execution. (Bug #21354)
- It was possible for a stored routine with a non-`latin1` name to cause a stack overrun. (Bug #21311)
- Certain malformed `INSERT` statements could crash the `mysql` client. (Bug #21142)
- Creating a `TEMPORARY` table with the same name as an existing table that was locked by another client could result in a lock conflict for `DROP TEMPORARY TABLE` because the server unnecessarily tried to acquire a name lock. (Bug #21096)
- Incorrect results could be obtained from re-execution of a parametrized prepared statement or a stored routine with a `SELECT` that uses `LEFT JOIN` with a second table having only one row. (Bug #21081)
- Within a stored routine, a view definition cannot refer to routine parameters or local variables. However, an error did not occur until the routine was called. Now it occurs during parsing of the routine creation statement.

**Note**

A side effect of this fix is that if you have already created such routines, and error will occur if you execute `SHOW CREATE PROCEDURE` or `SHOW CREATE FUNCTION`. You should drop these routines because they are erroneous.

(Bug #20953)

- In `mysql`, invoking `connect` or `\r` with very long `db_name` or `host_name` parameters caused buffer overflow. (Bug #20894)
- `SHOW VARIABLES` truncated the `Value` field to 256 characters. (Bug #20862)
- Selecting into variables sometimes returned incorrect wrong results. (Bug #20836)
- `WITH ROLLUP` could group unequal values. (Bug #20825)
- Range searches on columns with an index prefix could miss records. (Bug #20732)
- Inserting `DEFAULT` into a column with no default value could result in garbage in the column. Now the same result occurs as when inserting `NULL` into a `NOT NULL` column. (Bug #20691)
- An `UPDATE` that referred to a key column in the `WHERE` clause and activated a trigger that modified the column resulted in a loop. (Bug #20670)

- `CONCURRENT` did not work correctly for `LOAD DATA INFILE`. (Bug #20637)
- `mysql_fix_privilege_tables.sql` altered the `table_privs.table_priv` column to contain too few privileges, causing loss of the `CREATE VIEW` and `SHOW VIEW` privileges. (Bug #20589)
- `LIKE` searches failed for indexed `utf8` character columns. (Bug #20471)
- With `lower_case_table_names` set to 1, `SHOW CREATE TABLE` printed incorrect output for table names containing Turkish I (LATIN CAPITAL LETTER I WITH DOT ABOVE). (Bug #20404)
- A query with a subquery that references columns of a view from the outer `SELECT` could return an incorrect result if used from a prepared statement. (Bug #20327)
- For queries that select from a view, the server returned `MYSQL_FIELD` metadata inconsistently for view names and table names. For view columns, the server now returns the view name in the `table` field and, if the column selects from an underlying table, the table name in the `org_table` field. (Bug #20191)
- Invalidating the query cache caused a server crash for `INSERT INTO ... SELECT` statements that selected from a view. (Bug #20045)
- With `sql_mode = TRADITIONAL`, MySQL incorrectly aborted on warnings within stored routines and triggers. (Bug #20028)
- Unsigned `BIGINT` values treated as signed values by the `MOD()` function. (Bug #19955)
- Compiling PHP 5.1 with the MySQL static libraries failed on some versions of Linux. (Bug #19817)
- The `DELIMITER` statement did not work correctly when used in an SQL file run using the `SOURCE` statement. (Bug #19799)
- `mysqldump --xml` produced invalid XML for `BLOB` data. (Bug #19745)
- For a cast of a `DATETIME` value containing microseconds to `DECIMAL`, the microseconds part was truncated without generating a warning. Now the microseconds part is preserved. (Bug #19491)
- `InnoDB`: Reduced optimization level for Windows 64 builds to handle possible memory overrun. (Bug #19424)
- `VARBINARY` column values inserted on a MySQL 4.1 server had trailing zeros following upgrade to MySQL 5.0 or later. (Bug #19371)
- `FLUSH INSTANCES` in Instance Manager triggered an assertion failure. (Bug #19368)
- For a debug server, a reference to an undefined user variable in a prepared statement executed with `EXECUTE` caused an assertion failure. (Bug #19356)
- The server could send incorrect column count information to the client for queries that produce a larger number of columns than can fit in a two-byte number. (Bug #19216)
- Within a trigger for a base table, selecting from a view on that base table failed. (Bug #19111)
- The value of the `warning_count` system variable was not being calculated correctly (also affecting `SHOW COUNT(*) WARNINGS`). (Bug #19024)
- For some problems relating to character set conversion or incorrect string values for `INSERT` or `UPDATE`, the server reported truncation or length errors instead. (Bug #18908)
- `DELETE IGNORE` could hang for foreign key parent deletes. (Bug #18819)

- Constant expressions and some numeric constants used as input parameters to user-defined functions were not treated as constants. (Bug #18761)
- `InnoDB` used table locks (not row locks) within stored functions. (Bug #18077)
- `mysampack` wrote to unallocated memory, causing a crash. (Bug #17951)
- `FLUSH LOGS` or `mysqladmin flush-logs` caused a server crash if the binary log was not open. (Bug #17733)
- `mysql_fix_privilege_tables` did not accept a password containing embedded space or apostrophe characters. (Bug #17700)
- `mysql` would lose its connection to the server if its standard output was not writable. (Bug #17583)
- Attempting to use a view containing `DEFINER` information for a nonexistent user resulted in an error message that revealed the definer account. Now the definer is revealed only to users that have the `SUPER` privilege. Other users receive only an `access denied` message. (Bug #17254)
- `mysql-test-run` did not work correctly for RPM-based installations. (Bug #17194)
- `IN()` and `CHAR()` can return `NULL`, but did not signal that to the query processor, causing incorrect results for `IS NULL` operations. (Bug #17047)
- A client library crash was caused by executing a statement such as `SELECT * FROM t1 PROCEDURE ANALYSE()` using a server side cursor on a table `t1` that does not have the same number of columns as the output from `PROCEDURE ANALYSE()`. (Bug #17039)
- The `WITH CHECK OPTION` for a view failed to prevent storing invalid column values for `UPDATE` statements. (Bug #16813)
- `ALTER TABLE` was not able to rename a view. (Bug #14959)
- Statements such as `DROP PROCEDURE` and `DROP VIEW` were written to the binary log too late due to a race condition. (Bug #14262)
- A literal string in a `GROUP BY` clause could be interpreted as a column name. (Bug #14019)
- Instance Manager didn't close the client socket file when starting a new `mysqld` instance. `mysqld` inherited the socket, causing clients connected to Instance Manager to hang. (Bug #12751)
- Entries in the slow query log could have an incorrect `Rows_examined` value. (Bug #12240)
- Warnings were generated when explicitly casting a character to a number (for example, `CAST('x' AS SIGNED)`), but not for implicit conversions in simple arithmetic operations (such as `'x' + 0`). Now warnings are generated in all cases. (Bug #11927)
- Lack of validation for input and output `TIME` values resulted in several problems: `SEC_TO_TIME()` in some cases did not clip large values to the `TIME` range appropriately; `SEC_TO_TIME()` treated `BIGINT UNSIGNED` values as signed; only truncation warnings were produced when both truncation and out-of-range `TIME` values occurred. (Bug #11655, Bug #20927)
- Metadata for columns calculated from scalar subqueries was limited to integer, double, or string, even if the actual type of the column was different. (Bug #11032)
- Several string functions could return incorrect results when given very large length arguments. (Bug #10963)
- `FROM_UNIXTIME()` did not accept arguments up to `POWER(2, 31) - 1`, which it had previously. (Bug #9191)

- Subqueries of the form `NULL IN (SELECT ...)` returned invalid results. (Bug #8804, Bug #23485)
- `OPTIMIZE TABLE` with `myisam_repair_threads > 1` could result in `MyISAM` table corruption. (Bug #8283)

Changes in MySQL Enterprise 5.0.32 [MRU] (2006-12-20)

This is a *Monthly Rapid Update* release of the MySQL Enterprise Server 5.0.

This section documents all changes and bug fixes that have been applied since the last MySQL Enterprise Server release (5.0.30).

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- **Incompatible Change:** `InnoDB` rolls back only the last statement on a transaction timeout. A new option, `--innodb_rollback_on_timeout`, causes `InnoDB` to abort and roll back the entire transaction if a transaction timeout occurs (the same behavior as in MySQL 5.0.13 and earlier). (Bug #24200)
- **Incompatible Change:** The `prepared_stmt_count` system variable has been converted to the `Prepared_stmt_count` global status variable (viewable with the `SHOW GLOBAL STATUS` statement). (Bug #23159)
- **MySQL Cluster:** Setting the configuration parameter `LockPagesInMainMemory` had no effect. (Bug #24461)
- **MySQL Cluster:** It is now possible to create a unique hashed index on a column that is not defined as `NOT NULL`.



Note

This change applies only to tables using the `NDB` storage engine.

Unique indexes on columns in `NDB` tables do not store null values because they are mapped to primary keys in an internal index table (and primary keys cannot contain nulls).

Normally, an additional ordered index is created when one creates unique indexes on `NDB` table columns; this can be used to search for `NULL` values. However, if `USING HASH` is specified when such an index is created, no ordered index is created.

The reason for permitting unique hash indexes with null values is that, in some cases, the user wants to save space if a large number of records are pre-allocated but not fully initialized. This also assumes that the user will *not* try to search for null values. Since MySQL does not support indexes that are not permitted to be searched in some cases, the `NDB` storage engine uses a full table scan with pushed conditions for the referenced index columns to return the correct result.

A warning is returned if one creates a unique nullable hash index, since the query optimizer should be provided a hint not to use it with `NULL` values if this can be avoided. (Bug #21507)

- `DROP TRIGGER` now supports an `IF EXISTS` clause. (Bug #23703)
- The `Com_create_user` status variable was added (for counting `CREATE USER` statements). (Bug #22958)

- The `--memlock` option relies on system calls that are unreliable on some operating systems. If a crash occurs, the server now checks whether `--memlock` was specified and if so issues some information about possible workarounds. (Bug #22860)
- `mysqldump` now accepts the `--debug-info` option, which displays debugging information and memory and CPU usage statistics at program exit.
- The bundled yaSSL library was upgraded to version 1.5.0.

Bugs Fixed

- **Performance:** The `InnoDB` mutex structure was simplified to reduce memory load. (Bug #24386)
- **Performance:** Evaluation of subqueries that require the filesort algorithm were allocating and freeing the `sort_buffer_size` buffer many times, resulting in slow performance. Now the buffer is allocated once and reused. (Bug #21727)
- **MySQL Cluster:** The failure of a data node failure during a schema operation could lead to additional node failures. (Bug #24752)
- **MySQL Cluster:** A committed read could be attempted before a data node had time to connect, causing a timeout error. (Bug #24717)
- **MySQL Cluster:** Sudden disconnection of an SQL or data node could lead to shutdown of data nodes with the error `failed ndbrequire`. (Bug #24447)
- **MySQL Cluster:** `ndb_config` failed when trying to use 2 management servers and node IDs. (Bug #23887)
- **MySQL Cluster:** If the value set for `MaxNoOfAttributes` is excessive, a suitable error message is now returned. (Bug #19352)
- **MySQL Cluster:** A unique constraint violation was not ignored by an `UPDATE IGNORE` statement when the constraint violation occurred on a nonprimary key. (Bug #18487, Bug #24303)
- **Replication:** Changes to character set variables prior to an action on a replication-ignored table were forgotten by slave servers. (Bug #22877)
- **Replication:** On slave servers, transactions that exceeded the lock wait timeout failed to roll back properly. (Bug #20697)
- **Replication:** SQL statements close to the size of `max_allowed_packet` could produce binary log events larger than `max_allowed_packet` that could not be read by slave servers. (Bug #19402)
- **Replication:** Slave servers would retry the execution of an SQL statement an infinite number of times, ignoring the value `SLAVE_TRANSACTION_RETRIES` when using the NDB engine. (Bug #16228)
- **Cluster API:** Using `BIT` values with any of the comparison methods of the `NdbScanFilter` class caused data nodes to fail. (Bug #24503)
- **Cluster API:** Some MGM API function calls could yield incorrect return values in certain cases where the cluster was operating under a very high load, or experienced timeouts in inter-node communications. (Bug #24011)
- The `REPEAT()` function could return `NULL` when passed a column for the count argument. (Bug #24947)
- `mysql_upgrade` failed if the `--password` (or `-p`) option was given. (Bug #24896)
- With `innodb_file_per_table` enabled, `InnoDB` displayed incorrect file times in the output from `SHOW TABLE STATUS`. (Bug #24712)

- `ALTER TABLE ENABLE KEYS` or `ALTER TABLE DISABLE KEYS` combined with another `ALTER TABLE` option other than `RENAME TO` did nothing. In addition, if `ALTER TABLE` was used on a table having disabled keys, the keys of the resulting table were enabled. (Bug #24395)
- The `--extern` option for `mysql-test-run.pl` did not function correctly. (Bug #24354)
- Foreign key identifiers for `InnoDB` tables could not contain certain characters. (Bug #24299)
- The `mysql.server` script used the `source` command, which is less portable than the `.` command; it now uses `.` instead. (Bug #24294)
- `ALTER TABLE` statements that performed both `RENAME TO` and `{ENABLE|DISABLE} KEYS` operations caused a server crash. (Bug #24219)
- The loose index scan optimization for `GROUP BY` with `MIN` or `MAX` was not applied within other queries, such as `CREATE TABLE ... SELECT ...`, `INSERT ... SELECT ...`, or in the `FROM` clauses of subqueries. (Bug #24156)
- Subqueries for which a pushed-down condition did not produce exactly one key field could cause a server crash. (Bug #24056)
- The size of `MEMORY` tables and internal temporary tables was limited to 4GB on 64-bit Windows systems. (Bug #24052)
- `ROW_COUNT()` did not work properly as an argument to a stored procedure. (Bug #23760)
- `LAST_DAY('0000-00-00')` could cause a server crash. (Bug #23653)
- A trigger that invoked a stored function could cause a server crash when activated by different client connections. (Bug #23651)
- The stack size for NetWare binaries was increased to 128KB to prevent problems caused by insufficient stack size. (Bug #23504)
- If elements in a nontop-level `IN` subquery were accessed by an index and the subquery result set included a `NULL` value, the quantified predicate that contained the subquery was evaluated to `NULL` when it should return a non-`NULL` value. (Bug #23478)
- When applying the `group_concat_max_len` limit, `GROUP_CONCAT()` could truncate multibyte characters in the middle. (Bug #23451)
- `mysql_affected_rows()` could return values different from `mysql_stmt_affected_rows()` for the same sequence of statements. (Bug #23383)
- Accuracy was improved for comparisons between `DECIMAL` columns and numbers represented as strings. (Bug #23260)
- Calculation of `COUNT(DISTINCT)`, `AVG(DISTINCT)`, or `SUM(DISTINCT)` when they are referenced more than once in a single query with `GROUP BY` could cause a server crash. (Bug #23184)
- Queries using a column alias in an expression as part of an `ORDER BY` clause failed, an example of such a query being `SELECT mycol + 1 AS mynum FROM mytable ORDER BY 30 - mynum`. (Bug #22457)
- Using `EXPLAIN` caused a server crash for queries that selected from `INFORMATION_SCHEMA` in a subquery in the `FROM` clause. (Bug #22413)
- A server crash occurred when using `LOAD DATA` to load a table containing a `NOT NULL` spatial column, when the statement did not load the spatial column. Now a `NULL supplied to NOT NULL column` error occurs. (Bug #22372)

- `DATE_ADD()` requires complete dates with no “zero” parts, but sometimes did not return `NULL` when given such a date. (Bug #22229)
- Some small double precision numbers (such as `1.00000001e-300`) that should have been accepted were truncated to zero. (Bug #22129)
- For a nonexistent table, `DROP TEMPORARY TABLE` failed with an incorrect error message if `read_only` was enabled. (Bug #22077)
- Trailing spaces were not removed from Unicode `CHAR` column values when used in indexes. This resulted in excessive usage of storage space, and could affect the results of some `ORDER BY` queries that made use of such indexes.

**Note**

When upgrading, it is necessary to re-create any existing indexes on Unicode `CHAR` columns of each affected table to take advantage of the fix. See [Rebuilding or Repairing Tables or Indexes](#).

(Bug #22052)

- `STR_TO_DATE()` returned `NULL` if the format string contained a space following a nonformat character. (Bug #22029)
- In some cases, the parser failed to distinguish a user-defined function from a stored function. (Bug #21809)
- Inserting a default or invalid value into a spatial column could fail with `Unknown error` rather than a more appropriate error. (Bug #21790)
- It was possible to use `DATETIME` values whose year, month, and day parts were all zeros but whose hour, minute, and second parts contained nonzero values, an example of such an illegal `DATETIME` being `'0000-00-00 11:23:45'`.

**Note**

This fix was reverted in MySQL 5.0.40.

(Bug #21789)

References: See also: Bug #25301.

- yaSSL crashed on pre-Pentium Intel CPUs. (Bug #21765)
- Through the C API, the member strings in `MYSQL_FIELD` for a query that contained expressions could return incorrect results. (Bug #21635)
- Using `FLUSH TABLES` in one connection while another connection is using `HANDLER` statements caused a server crash.

**Note**

This fix was reverted in MySQL 5.0.48

(Bug #21587)

References: See also: Bug #29474.

- View columns were always handled as having implicit derivation, leading to `illegal mix of collation errors` for some views in `UNION` operations. Now view column derivation comes from the original expression given in the view definition. (Bug #21505)
- `InnoDB` crashed while performing XA recovery of prepared transactions. (Bug #21468)
- `INET_ATON()` returned a signed `BIGINT` value, not an unsigned value. (Bug #21466)
- It was possible to set the backslash character (“\”) as the delimiter character using `DELIMITER`, but not actually possible to use it as the delimiter. (Bug #21412)
- Selecting into variables sometimes returned incorrect wrong results. (Bug #20836)
- `CONCURRENT` did not work correctly for `LOAD DATA INFILE`. (Bug #20637)
- `mysql_fix_privilege_tables.sql` altered the `table_privs.table_priv` column to contain too few privileges, causing loss of the `CREATE VIEW` and `SHOW VIEW` privileges. (Bug #20589)
- With `lower_case_table_names` set to 1, `SHOW CREATE TABLE` printed incorrect output for table names containing Turkish I (LATIN CAPITAL LETTER I WITH DOT ABOVE). (Bug #20404)
- A query with a subquery that references columns of a view from the outer `SELECT` could return an incorrect result if used from a prepared statement. (Bug #20327)
- For queries that select from a view, the server returned `MYSQL_FIELD` metadata inconsistently for view names and table names. For view columns, the server now returns the view name in the `table` field and, if the column selects from an underlying table, the table name in the `org_table` field. (Bug #20191)
- Invalidating the query cache caused a server crash for `INSERT INTO ... SELECT` statements that selected from a view. (Bug #20045)
- Unsigned `BIGINT` values treated as signed values by the `MOD()` function. (Bug #19955)
- Compiling PHP 5.1 with the MySQL static libraries failed on some versions of Linux. (Bug #19817)
- The `DELIMITER` statement did not work correctly when used in an SQL file run using the `SOURCE` statement. (Bug #19799)
- For a cast of a `DATETIME` value containing microseconds to `DECIMAL`, the microseconds part was truncated without generating a warning. Now the microseconds part is preserved. (Bug #19491)
- `VARBINARY` column values inserted on a MySQL 4.1 server had trailing zeros following upgrade to MySQL 5.0 or later. (Bug #19371)
- The server could send incorrect column count information to the client for queries that produce a larger number of columns than can fit in a two-byte number. (Bug #19216)
- For some problems relating to character set conversion or incorrect string values for `INSERT` or `UPDATE`, the server reported truncation or length errors instead. (Bug #18908)
- Constant expressions and some numeric constants used as input parameters to user-defined functions were not treated as constants. (Bug #18761)
- `myisampack` wrote to unallocated memory, causing a crash. (Bug #17951)
- `FLUSH LOGS` or `mysqladmin flush-logs` caused a server crash if the binary log was not open. (Bug #17733)

- `mysql_fix_privilege_tables` did not accept a password containing embedded space or apostrophe characters. (Bug #17700)
- Attempting to use a view containing `DEFINER` information for a nonexistent user resulted in an error message that revealed the definer account. Now the definer is revealed only to users that have the `SUPER` privilege. Other users receive only an `access denied` message. (Bug #17254)
- `IN()` and `CHAR()` can return `NULL`, but did not signal that to the query processor, causing incorrect results for `IS NULL` operations. (Bug #17047)
- Warnings were generated when explicitly casting a character to a number (for example, `CAST('x' AS SIGNED)`), but not for implicit conversions in simple arithmetic operations (such as `'x' + 0`). Now warnings are generated in all cases. (Bug #11927)
- Metadata for columns calculated from scalar subqueries was limited to integer, double, or string, even if the actual type of the column was different. (Bug #11032)
- Subqueries of the form `NULL IN (SELECT ...)` returned invalid results. (Bug #8804, Bug #23485)

Changes in MySQL Enterprise 5.0.30sp1 [QSP] (2007-01-19)

This is a *Service Pack* release of the MySQL Enterprise Server 5.0.

This section documents all changes and bug fixes that have been applied since the last MySQL Enterprise Server release (5.0.30).

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- **Incompatible Change:** `InnoDB` rolls back only the last statement on a transaction timeout. A new option, `--innodb_rollback_on_timeout`, causes `InnoDB` to abort and roll back the entire transaction if a transaction timeout occurs (the same behavior as in MySQL 5.0.13 and earlier). (Bug #24200)

Bugs Fixed

- **Performance:** Evaluation of subqueries that require the filesort algorithm were allocating and freeing the `sort_buffer_size` buffer many times, resulting in slow performance. Now the buffer is allocated once and reused. (Bug #21727)
- **Replication:** A stored procedure, executed from a connection using a binary character set, and which wrote multibyte data, would write incorrectly escaped entries to the binary log. This caused syntax errors, and caused replication to fail. (Bug #23619, Bug #24492)
- The loose index scan optimization for `GROUP BY` with `MIN` or `MAX` was not applied within other queries, such as `CREATE TABLE ... SELECT ...`, `INSERT ... SELECT ...`, or in the `FROM` clauses of subqueries. (Bug #24156)
- The size of `MEMORY` tables and internal temporary tables was limited to 4GB on 64-bit Windows systems. (Bug #24052)
- Accuracy was improved for comparisons between `DECIMAL` columns and numbers represented as strings. (Bug #23260)
- Calculation of `COUNT(DISTINCT)`, `AVG(DISTINCT)`, or `SUM(DISTINCT)` when they are referenced more than once in a single query with `GROUP BY` could cause a server crash. (Bug #23184)

- [InnoDB](#) crashed while performing XA recovery of prepared transactions. (Bug #21468)
- Certain malformed [INSERT](#) statements could crash the [mysql](#) client. (Bug #21142)
- [CONCURRENT](#) did not work correctly for [LOAD DATA INFILE](#). (Bug #20637)
- Several string functions could return incorrect results when given very large length arguments. (Bug #10963)

Changes in MySQL Enterprise 5.0.30 [MRU] (2006-11-14)

This is a *Monthly Rapid Update* release of the MySQL Enterprise Server 5.0.

This section documents all changes and bug fixes that have been applied since the last MySQL Enterprise Server release (5.0.28).

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- **MySQL Cluster:** The [ndb_config](#) utility now accepts `-c` as a short form of the `--ndb-connectstring` option. (Bug #22295)
- **MySQL Cluster:** Added the `--bind-address` option for [ndbd](#). This permits a data node process to be bound to a specific network interface. (Bug #22195)
- **MySQL Cluster:** The [NDB](#) storage engine could leak memory during file operations. (Bug #21858)
- **MySQL Cluster:** The [Ndb_number_of_storage_nodes](#) system variable was renamed to [Ndb_number_of_data_nodes](#). (Bug #20848)
- **MySQL Cluster:** The [HELP](#) command in the Cluster management client now provides command-specific help. For example, `HELP RESTART` in [ndb_mgm](#) provides detailed information about the [RESTART](#) command. (Bug #19620)
- If the user specified the server options `--max-connections=N` or `--table-cache=M`, a warning would be given in some cases that some values were recalculated, with the result that `--table-cache` could be assigned greater value.

In such cases, both the warning and the increase in the `--table-cache` value were completely harmless. Note also that it is not possible for the MySQL Server to predict or to control limitations on the maximum number of open files, since this is determined by the operating system.

The value of `--table-cache` is no longer increased automatically, and a warning is now given only if some values had to be decreased due to operating system limits. (Bug #21915)

- For the [CALL](#) statement, stored procedures that take no arguments now can be invoked without parentheses. That is, `CALL p()` and `CALL p` are equivalent. (Bug #21462)
- [mysql_upgrade](#) now passes all the parameters specified on the command line to both [mysqlcheck](#) and [mysql](#) using the [upgrade_defaults](#) file. (Bug #20100)
- [SHOW STATUS](#) is no longer logged to the slow query log. (Bug #19764)
- [mysqldump](#) `--single-transaction` now uses `START TRANSACTION /*!40100 WITH CONSISTENT SNAPSHOT */` rather than `BEGIN` to start a transaction, so that a consistent snapshot will be used on those servers that support it. (Bug #19660)

Bugs Fixed

- **Performance:** [InnoDB](#) exhibited thread thrashing with more than 50 concurrent connections under an update-intensive workload. (Bug #22868)
- **Performance:** [InnoDB](#) showed substandard performance with multiple queries running concurrently. (Bug #15815)
- **MySQL Cluster:** Backup of a cluster failed if there were any tables with 128 or more columns. (Bug #23502)
- **MySQL Cluster:** Cluster backups failed when there were more than 2048 schema objects in the cluster. (Bug #23499)
- **MySQL Cluster:** The management client command `ALL DUMP 1000` would cause the cluster to crash if data nodes were connected to the cluster but not yet fully started. (Bug #23203)
- **MySQL Cluster:** `INSERT ... ON DUPLICATE KEY UPDATE` on an [NDB](#) table could lead to deadlocks and memory leaks. (Bug #23200)
- **MySQL Cluster:** (NDB API): Inactivity timeouts for scans were not correctly handled. (Bug #23107)
- **MySQL Cluster:** If a node restart could not be performed from the REDO log, no node takeover took place. This could cause partitions to be left empty during a system restart. (Bug #22893)
- **MySQL Cluster:** Multiple node restarts in rapid succession could cause a system restart to fail , or induce a race condition. (Bug #22892, Bug #23210)
- **MySQL Cluster:** (NDB API): Attempting to read a nonexistent tuple using `Commit` mode for `NdbTransaction::execute()` caused node failures. (Bug #22672)
- **MySQL Cluster:** The `--help` output from [NDB](#) binaries did not include file-related options. (Bug #21994)
- **MySQL Cluster:** (NDB API): Scans closed before being executed were still placed in the send queue. (Bug #21941)
- **MySQL Cluster:** A scan timeout returned Error 4028 (`Node failure caused abort of transaction`) instead of Error 4008 (`Node failure caused abort of transaction...`). (Bug #21799)
- **MySQL Cluster:** The node recovery algorithm was missing a version check for tables in the `ALTER_TABLE_COMMITTED` state (as opposed to the `TABLE_ADD_COMMITTED` state, which has the version check). This could cause inconsistent schemas across nodes following node recovery. (Bug #21756)
- **MySQL Cluster:** Partition distribution keys were updated only for the primary and starting replicas during node recovery. This could lead to node failure recovery for clusters having an odd number of replicas.

**Note**

For best results, use values for `NumberOfReplicas` that are even powers of 2.

(Bug #21535)

- **MySQL Cluster:** The `ndb_mgm` management client did not set the exit status on errors, always returning 0 instead. (Bug #21530)
- **MySQL Cluster:** Attempting to create an [NDB](#) table on a MySQL with an existing non-Cluster table with the same name in the same database could result in data loss or corruption. MySQL now issues

a warning when a `SHOW TABLES` or other statement causing table discovery finds such a table. (Bug #21378)

- **MySQL Cluster:** Cluster logs were not rotated following the first rotation cycle. (Bug #21345)
- **MySQL Cluster:** When inserting a row into an `NDB` table with a duplicate value for a nonprimary unique key, the error issued would reference the wrong key. (Bug #21072)
- **MySQL Cluster:** Condition pushdown did not work correctly with `DATETIME` columns. (Bug #21056)
- **MySQL Cluster:** Under some circumstances, local checkpointing would hang, keeping any unstarted nodes from being started. (Bug #20895)
- **MySQL Cluster:** Using an invalid node ID with the management client `STOP` command could cause `ndb_mgm` to hang. (Bug #20575)
- **MySQL Cluster:** Data nodes added while the cluster was running in single user mode were all assigned node ID 0, which could later cause multiple node failures. Adding nodes while in single user mode is no longer possible. (Bug #20395)
- **MySQL Cluster:** In some cases where `SELECT COUNT(*)` from an `NDB` table should have yielded an error, `MAX_INT` was returned instead. (Bug #19914)
- **MySQL Cluster:** Following the restart of a management node, the Cluster management client did not automatically reconnect. (Bug #19873)
- **MySQL Cluster:** Error messages given when trying to make online changes to parameters such as `NoOfReplicas` that can only be changed using a complete shutdown and restart of the cluster did not indicate the true nature of the problem. (Bug #19787)
- **MySQL Cluster:** `ndb_restore` did not always make clear that it had recovered successfully from temporary errors while restoring a cluster backup. (Bug #19651)
- **MySQL Cluster:** In rare situations with resource shortages, a crash could result from an insufficient number of `IndexScanOperation` objects. (Bug #19198)
- **MySQL Cluster:** `ndb_mgm -e show | head` would hang after displaying the first 10 lines of output. (Bug #19047)
- **MySQL Cluster:** The error returned by the cluster when too many nodes were defined did not make clear the nature of the problem. (Bug #19045)
- **MySQL Cluster:** The `ndb_config` utility did not perform host lookups correctly when using the `--host` option (Bug #17582)
- **MySQL Cluster:** A problem with takeover during a system restart caused ordered indexes to be rebuilt incorrectly. (Bug #15303)
- **Replication:** Column names were not quoted properly for replicated views. (Bug #19736)
- **Replication:** Transient errors in replication from master to slave may trigger multiple `Got fatal error 1236: 'binlog truncated in the middle of event'` errors on the slave. (Bug #4053)
- **Cluster API:** The `NdbOperation::getBlobHandle()` method, when called with the name of a nonexistent column, caused a segmentation fault. (Bug #21036)
- **Cluster API:** When multiple processes or threads in parallel performed the same ordered scan with exclusive lock and updated the retrieved records, the scan could skip some records, which as a result were not updated. (Bug #20446)

- There was a race condition in the `InnoDB fil_flush_file_spaces()` function. (Bug #24089)
References: This issue is a regression of: Bug #15653.
- yaSSL-related memory leaks were detected by Valgrind. (Bug #23981)
- The internal SQL interpreter of `InnoDB` placed an unnecessary lock on the supremum record with `innodb_locks_unsafe_for_binlog` enabled. This caused an assertion failure when `InnoDB` was built with debugging enabled. (Bug #23769)
- `M % 0` returns `NULL`, but `(M % 0) IS NULL` evaluated to false. (Bug #23411)
- For not-yet-authenticated connections, the `Time` column in `SHOW PROCESSLIST` was a random value rather than `NULL`. (Bug #23379)
- MySQL failed to build on Linux/Alpha. (Bug #23256)
References: This issue is a regression of: Bug #21250.
- If `COMPRESS()` returned `NULL`, subsequent invocations of `COMPRESS()` within a result set or within a trigger also returned `NULL`. (Bug #23254)
- Insufficient memory (`myisam_sort_buffer_size`) could cause a server crash for several operations on `MyISAM` tables: repair table, create index by sort, repair by sort, parallel repair, bulk insert. (Bug #23175)
- The column default value in the output from `SHOW COLUMNS` or `SELECT FROM INFORMATION_SCHEMA.COLUMNS` was truncated to 64 characters. (Bug #23037)
- `mysql` did not check for errors when fetching data during result set printing. (Bug #22913)
- The return value from `my_seek()` was ignored. (Bug #22828)
- The optimizer failed to use equality propagation for `BETWEEN` and `IN` predicates with string arguments. (Bug #22753)
- The `Handler_rollback` status variable sometimes was incremented when no rollback had taken place. (Bug #22728)
- The `Host` column in `SHOW PROCESSLIST` output was blank when the server was started with the `--skip-grant-tables` option. (Bug #22723)
- If a table contains an `AUTO_INCREMENT` column, inserting into an insertable view on the table that does not include the `AUTO_INCREMENT` column should not change the value of `LAST_INSERT_ID()`, because the side effects of inserting default values into columns not part of the view should not be visible. MySQL was incorrectly setting `LAST_INSERT_ID()` to zero. (Bug #22584)
- Instance Manager had a race condition involving `mysqld` PID file removal. (Bug #22379)
- The optimizer used the `ref` join type rather than `eq_ref` for a simple join on strings. (Bug #22367)
- Some queries that used `MAX()` and `GROUP BY` could incorrectly return an empty result. (Bug #22342)
- If an `init_connect` SQL statement produced an error, the connection was silently terminated with no error message. Now the server writes a warning to the error log. (Bug #22158)
- Use of a DES-encrypted SSL certificate file caused a server crash. (Bug #21868)
- Use of `PREPARE` with a `CREATE PROCEDURE` statement that contained a syntax error caused a server crash. (Bug #21856)

- Adding a day, month, or year interval to a `DATE` value produced a `DATE`, but adding a week interval produced a `DATETIME` value. Now all produce a `DATE` value. (Bug #21811)
- Use of a subquery that invoked a function in the column list of the outer query resulted in a memory leak. (Bug #21798)
- Selecting from a `MERGE` table could result in a server crash if the underlying tables had fewer indexes than the `MERGE` table itself. (Bug #21617, Bug #22937)
- After `FLUSH TABLES WITH READ LOCK` followed by `UNLOCK TABLES`, attempts to drop or alter a stored routine failed with an error that the routine did not exist, and attempts to execute the routine failed with a lock conflict error. (Bug #21414)
- For multiple-table `UPDATE` statements, storage engines were not notified of duplicate-key errors. (Bug #21381)
- Within a prepared statement, `SELECT (COUNT(*) = 1)` (or similar use of other aggregate functions) did not return the correct result for statement re-execution. (Bug #21354)
- It was possible for a stored routine with a non-`latin1` name to cause a stack overrun. (Bug #21311)
- Creating a `TEMPORARY` table with the same name as an existing table that was locked by another client could result in a lock conflict for `DROP TEMPORARY TABLE` because the server unnecessarily tried to acquire a name lock. (Bug #21096)
- Incorrect results could be obtained from re-execution of a parametrized prepared statement or a stored routine with a `SELECT` that uses `LEFT JOIN` with a second table having only one row. (Bug #21081)
- Within a stored routine, a view definition cannot refer to routine parameters or local variables. However, an error did not occur until the routine was called. Now it occurs during parsing of the routine creation statement.

**Note**

A side effect of this fix is that if you have already created such routines, an error will occur if you execute `SHOW CREATE PROCEDURE` or `SHOW CREATE FUNCTION`. You should drop these routines because they are erroneous.

(Bug #20953)

- In `mysql`, invoking `connect` or `\r` with very long `db_name` or `host_name` parameters caused buffer overflow. (Bug #20894)
- `SHOW VARIABLES` truncated the `Value` field to 256 characters. (Bug #20862)
- `WITH ROLLUP` could group unequal values. (Bug #20825)
- Range searches on columns with an index prefix could miss records. (Bug #20732)
- An `UPDATE` that referred to a key column in the `WHERE` clause and activated a trigger that modified the column resulted in a loop. (Bug #20670)
- `LIKE` searches failed for indexed `utf8` character columns. (Bug #20471)
- With `sql_mode = TRADITIONAL`, MySQL incorrectly aborted on warnings within stored routines and triggers. (Bug #20028)
- `mysqldump --xml` produced invalid XML for `BLOB` data. (Bug #19745)

- `FLUSH INSTANCES` in Instance Manager triggered an assertion failure. (Bug #19368)
- For a debug server, a reference to an undefined user variable in a prepared statement executed with `EXECUTE` caused an assertion failure. (Bug #19356)
- Within a trigger for a base table, selecting from a view on that base table failed. (Bug #19111)
- The value of the `warning_count` system variable was not being calculated correctly (also affecting `SHOW COUNT(*) WARNINGS`). (Bug #19024)
- `DELETE IGNORE` could hang for foreign key parent deletes. (Bug #18819)
- `InnoDB` used table locks (not row locks) within stored functions. (Bug #18077)
- `mysql` would lose its connection to the server if its standard output was not writable. (Bug #17583)
- `mysql-test-run` did not work correctly for RPM-based installations. (Bug #17194)
- A client library crash was caused by executing a statement such as `SELECT * FROM t1 PROCEDURE ANALYSE()` using a server side cursor on a table `t1` that does not have the same number of columns as the output from `PROCEDURE ANALYSE()`. (Bug #17039)
- The `WITH CHECK OPTION` for a view failed to prevent storing invalid column values for `UPDATE` statements. (Bug #16813)
- `ALTER TABLE` was not able to rename a view. (Bug #14959)
- Statements such as `DROP PROCEDURE` and `DROP VIEW` were written to the binary log too late due to a race condition. (Bug #14262)
- A literal string in a `GROUP BY` clause could be interpreted as a column name. (Bug #14019)
- Instance Manager didn't close the client socket file when starting a new `mysqld` instance. `mysqld` inherited the socket, causing clients connected to Instance Manager to hang. (Bug #12751)
- Entries in the slow query log could have an incorrect `Rows_examined` value. (Bug #12240)
- Lack of validation for input and output `TIME` values resulted in several problems: `SEC_TO_TIME()` in some cases did not clip large values to the `TIME` range appropriately; `SEC_TO_TIME()` treated `BIGINT UNSIGNED` values as signed; only truncation warnings were produced when both truncation and out-of-range `TIME` values occurred. (Bug #11655, Bug #20927)
- A locking safety check in `InnoDB` reported a spurious error `stored_select_lock_type is 0 inside ::start_stmt()` for `INSERT ... SELECT` statements in `innodb_locks_unsafe_for_binlog` mode. The safety check was removed. (Bug #10746)
- `FROM_UNIXTIME()` did not accept arguments up to `POWER(2, 31) - 1`, which it had previously. (Bug #9191)
- `OPTIMIZE TABLE` with `myisam_repair_threads > 1` could result in `MyISAM` table corruption. (Bug #8283)

Changes in MySQL Enterprise 5.0.28 (2006-10-24)

This is the first *MySQL Enterprise Server* release, following the last *Community Server* release (5.0.27).

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- Binary MySQL distributions no longer include a `mysqld-max` server, except for RPM distributions. Instead, distributions contain a `mysqld` binary that includes the features previously included in the `mysqld-max` binary.

Bugs Fixed

- MySQL 5.0.26 introduced an ABI incompatibility, which this release reverts. Programs compiled against 5.0.26 are not compatible with any other version and must be recompiled. (Bug #23427)
- **InnoDB**: Reduced optimization level for Windows 64 builds to handle possible memory overrun. (Bug #19424)

Changes in MySQL Community Server 5.0.27 (2006-10-21)

This is a bugfix release for the current MySQL Community Server production release family. It replaces MySQL 5.0.26.

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- This is the last version for which binary MySQL-Max distributions are available, except for RPM distributions. (For RPM distributions, the last version is 5.0.37.)

Bugs Fixed

- MySQL 5.0.26 introduced an ABI incompatibility, which this release reverts. Programs compiled against 5.0.26 are not compatible with any other version and must be recompiled. (Bug #23427)

Changes in MySQL 5.0.26 (2006-10-03)

This is a bugfix release for the current production release family.

This section documents all changes and bug fixes that have been applied since the last official MySQL release. If you would like to receive more fine-grained and personalized *update alerts* about fixes that are relevant to the version and features you use, please consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details, please see (<http://www.mysql.com/products/enterprise>).

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- **Important Change; MySQL Cluster:** `LOAD DATA INFILE` no longer causes an implicit commit for all storage engines. It now causes an implicit commit only for tables using the **NDB** storage engine. (Bug #11151)
- The number of **InnoDB** threads is no longer limited to 1,000 on Windows. (Bug #22268)
- `mysqldump` now has a `--flush-privileges` option. It causes `mysqldump` to emit a `FLUSH PRIVILEGES` statement after dumping the `mysql` database. This option should be used any time the dump contains the `mysql` database and any other database that depends on the data in the `mysql` database for proper restoration. (Bug #21424)

- For `mysqldump`, the output generated by the server when using the `--xml` option has changed with regard to null values. It now matches the output from `mysqldump --xml`. That is, a column containing a `NULL` value is now reported as

```
<field name="column_name" xsi:nil="true" />
```

whereas a column containing the string value `'NULL'` is reported as

```
<field name="column_name">NULL</field>
```

and a column containing an empty string is reported as

```
<field name="column_name"></field>
```

(Bug #21263)

- The source distribution has been updated so that the UDF example can be compiled under Windows with `CMake`. See [UDF Compiling and Installing](#). (Bug #19121)
- The `LOAD DATA FROM MASTER` and `LOAD TABLE FROM MASTER` statements are deprecated. See [LOAD DATA FROM MASTER Syntax](#), for recommended alternatives. (Bug #9125, Bug #20596, Bug #14399, Bug #12187, Bug #15025, Bug #18822)

Bugs Fixed

- **Replication:** Column names supplied for a view created on a master server could be lost on a slave server. (Bug #19419)
- Deleting entries from a large `MyISAM` index could cause index corruption when it needed to shrink. Deletes from an index can happen when a record is deleted, when a key changes and must be moved, and when a key must be un-inserted because of a duplicate key. This can also happen in `REPAIR TABLE` when a duplicate key is found and in `myisamchk` when sorting the records by an index. (Bug #22384)
- `yaSSL` had a conflicting definition for `socklen_t` on `hur-d-i386` systems. (Bug #22326)
- Conversion of values inserted into a `BIT` column could affect adjacent columns. (Bug #22271)
- `mysql_com.h` unnecessarily referred to the `ulong` type. (Bug #22227)
- The source distribution would not build on Windows due to a spurious dependency on `ib_config.h`. (Bug #22224)
- Execution of a prepared statement that uses an `IN` subquery with aggregate functions in the `HAVING` clause could cause a server crash. (Bug #22085)
- Using `GROUP_CONCAT()` on the result of a subquery in the `FROM` clause that itself used `GROUP_CONCAT()` could cause a server crash. (Bug #22015)
- A query that used `GROUP BY` and an `ALL` or `ANY` quantified subquery in a `HAVING` clause could trigger an assertion failure. (Bug #21853)
- `UPGRADE` was treated as a reserved word, although it is not. (Bug #21772)
- The value of `LAST_INSERT_ID()` was not always updated correctly within stored routines. (Bug #21726)

- A function result in a comparison was replaced with a constant by the optimizer under some circumstances when this optimization was invalid. (Bug #21698)
- If `mysqld` was linked against a system-installed `zlib` library compiled without large-file support, it would likely exit with a `SIGXFSZ` (file size exceeded) signal if an `ARCHIVE` table reached 2GB. The server now checks for space before writing. (Bug #21675)
- The presence of a subquery in the `ON` clause of a join in a view definition prevented the `MERGE` algorithm from being used for the view in cases where it should be permitted. (Bug #21646)
- When records are merged from the insert buffer and the page needs to be reorganized, `InnoDB` used incorrect column length information when interpreting the records of the page. This caused a server crash due to apparent corruption of secondary indexes in `ROW_FORMAT=COMPACT` that contain prefix indexes of fixed-length columns. Data files should not be corrupted, but the crash was likely to repeat every time the server was restarted. (Bug #21638)
- For character sets having a `mbmaxlen` value of 2, any `ALTER TABLE` statement changed `TEXT` columns to `MEDIUMTEXT`. (Bug #21620)
- `mysql` displayed an empty string for `NULL` values. (Bug #21618)
- For `INSERT ... ON DUPLICATE KEY UPDATE`, use of `VALUES(col_name)` within the `UPDATE` clause sometimes was handled incorrectly. (Bug #21555)
- Subqueries with aggregate functions but no `FROM` clause could return incorrect results. (Bug #21540)
- The server could crash for the second execution of a function containing a `SELECT` statement that uses an aggregating `IN` subquery. (Bug #21493)
- `myisam_ftdump` produced bad counts for common words. (Bug #21459)
- The URL into the online manual that is printed in the stack trace message by the server was out of date. (Bug #21449)
- Table aliases in multiple-table `DELETE` statements sometimes were not resolved. (Bug #21392)
- `mysql_config --libmysqld-libs` did not produce any SSL options necessary for linking `libmysqld` with SSL support enabled. (Bug #21239)
- In the package of pre-built time zone tables that is available for download at <http://dev.mysql.com/downloads/timezones.html>, the tables now explicitly use the `utf8` character set so that they work the same way regardless of the system character set value. (Bug #21208)
- A subquery that uses an index for both the `WHERE` and `ORDER BY` clauses produced an empty result. (Bug #21180)
- `mysql_upgrade` produced a malformed `upgrade_defaults` file by overwriting the `[client]` group header with a `password` option. This prevented `mysqlcheck` from running successfully when invoked by `mysql_upgrade`. (Bug #21011)
- On Windows, inserting into a `MERGE` table after renaming an underlying `MyISAM` table caused a server crash. (Bug #20789)
- Within stored routines, some error messages were printed incorrectly. A nonnull-terminated string was passed to a message-printing routine that expected a null-terminated string. (Bug #20778)
- `INSERT DELAYED` did not honor `SET INSERT_ID` or the `auto_increment_*` system variables. (Bug #20627, Bug #20830)

- If the `auto_increment_offset` setting causes MySQL to generate a value larger than the column's maximum possible value, the `INSERT` statement is accepted in strict SQL mode, whereas but should fail with an error. (Bug #20573)
- User names have a maximum length of 16 characters (even if they contain multibyte characters), but were being truncated to 16 bytes. (Bug #20393)
- `PROCEDURE ANALYSE()` returned incorrect values of `M FLOAT(M, D)` and `DOUBLE(M, D)`. (Bug #20305)
- For a `MyISAM` table locked with `LOCK TABLES ...WRITE`, queries optimized using the `index_merge` method did not show rows inserted with the lock in place. (Bug #20256)
- `SUBSTRING()` results sometimes were stored improperly into a temporary table when multibyte character sets were used. (Bug #20204)
- For an `ENUM` column that used the `ucs2` character set, using `ALTER TABLE` to modify the column definition caused the default value to be lost. (Bug #20108)
- Join conditions using index prefixes on `utf8` columns of `InnoDB` tables incorrectly ignored rows where the length of the actual value was greater than the length of the index prefix. (Bug #19960)
- `make install` tried to build files that should already have been built by `make all`, causing a failure if installation was performed using a different account than the one used for the initial build. (Bug #19738)
- For a `MyISAM` table with a `FULLTEXT` index, compression with `myisampack` or a check with `myisamchk` after compression resulted in table corruption. (Bug #19702)
- The build process incorrectly tried to overwrite `sql/lex_hash.h`. This caused the build to fail when using a shadow link tree pointing to original sources that were owned by another account. (Bug #18888)
- Linking the `pthread` library to single-threaded MySQL libraries caused `dlopen()` to fail at runtime on HP-UX. (Bug #18267)
- The source distribution failed to compile when configured with the `--with-libwrap` option. (Bug #18246)
- Queries containing a subquery that used aggregate functions could return incorrect results. (Bug #16792)
- Row equalities (such as `WHERE (a,b) = (c,d)`) were not taken into account by the optimizer, resulting in slow query execution. Now they are treated as conjunctions of equalities between row elements. (Bug #16081)
- `BIN()`, `OCT()`, and `CONV()` did not work with BIT values. (Bug #15583)
- The parser rejected queries that selected from a table twice using a `UNION` within a subquery. The parser now supports arbitrary subquery, join, and parenthesis operations within `EXISTS` subqueries. A limitation still exists for scalar subqueries: If the subquery contains `UNION`, the first `SELECT` of the `UNION` cannot be within parentheses. For example, `SELECT (SELECT a FROM t1 UNION SELECT b FROM t2)` will work, but `SELECT ((SELECT a FROM t1) UNION (SELECT b FROM t2))` will not. (Bug #14654)
- On Mac OS X, zero-byte `read()` or `write()` calls to an SMB-mounted file system could return a nonstandard return value, leading to data corruption. Now such calls are avoided. (Bug #12620)
- The server returns a more informative error message when it attempts to open a `MERGE` table that has been defined to use non-`MyISAM` tables. (Bug #10974)

- With `TRADITIONAL` SQL mode, assignment of out-of-bound values and rounding of assigned values was done correctly, but assignment of the same numbers represented as strings sometimes was handled differently. (Bug #6147)
- On an `INSERT` into an updatable but noninsertable view, an error message was issued stating that the view was not updatable. Now the message says the view is not insertable-into. (Bug #5505)
- `EXPLAIN` sometimes returned an incorrect `select_type` for a `SELECT` from a view, compared to the `select_type` for the equivalent `SELECT` from the base table. (Bug #5500)
- Incorporated portability fixes into the definition of `__attribute__` in `my_global.h`. (Bug #2717)

Changes in MySQL 5.0.25 (2006-09-15)

This is a bugfix release for the current production release family. This version was released as MySQL Classic 5.0.25 to commercial customers only.

This section documents all changes and bug fixes that have been applied since the last official MySQL release. If you would like to receive more fine-grained and personalized *update alerts* about fixes that are relevant to the version and features you use, please consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details, please see (<http://www.mysql.com/products/enterprise>).

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- MySQL did not properly do stack dumps on `x86_64` and `i386/NPTL` systems. (Note that the initial fix for this problem was discovered not to be correct. Further work on the problem was undertaken only for MySQL 5.1 and up. See Bug #31891.) (Bug #21250)

References: See also: Bug #31891.

- The `mysqld` and `mysqlmanager` man pages have been reclassified from volume 1 to volume 8. (Bug #21220)
- `InnoDB` now honors `IGNORE INDEX`. Previously using `IGNORE INDEX` in cases where an index sort would be slower than a filesort had no effect when used with `InnoDB` tables.



Note

This fix was reverted in MySQL 5.0.26, and a new fix made in MySQL 5.0.40.

(Bug #21174)

- `TIMESTAMP` columns that are `NOT NULL` now are reported that way by `SHOW COLUMNS` and `INFORMATION_SCHEMA`. (Bug #20910)
- The MySQL distribution now compiles on UnixWare 7.13. (Bug #20190)
- `configure` now defines the symbol `DEBUG_ON` in `config.h` to indicate whether the source tree is configured to be compiled with debugging support. (Bug #19517)
- `mysql_upgrade` no longer reads the `[client]` option file group because it is not a client and did not understand client options such as `host`. Now it reads only the `[mysql_upgrade]` group. (Bug #19452)
- For `mysqlshow`, if a database name argument contains wildcard characters (such as “_”) but matches a single database name exactly, treat the name as a literal name. This enables a command such as

`mysqlshow information_schema` to work without having to escape the wildcard character. (Bug #19147)

- On Windows, typing **Control+C** while a query was running caused the `mysql` client to crash. Now it causes `mysql` to attempt to kill the current statement. If this cannot be done, or **Control+C** is typed again before the statement is killed, `mysql` exits. (In other words, `mysql`'s behavior with regard to **Control+C** is now the same as it is on Unix platforms.) (Bug #17926)

References: See also: Bug #1989.

- The `VIEW_DEFINITION` column of the `INFORMATION_SCHEMA VIEWS` table now contains information about the view algorithm. (Bug #16832)
- The bundled yaSSL library licensing has added a FLOSS exception similar to MySQL to resolve licensing incompatibilities with MySQL. (See the `extra/yassl/FLOSS-EXCEPTIONS` file in a MySQL source distribution for details.) (Bug #16755)
- Table comments longer than 60 characters and column comments longer than 255 characters were truncated silently. Now a warning is issued, or an error in strict mode. (Bug #13934)
- The `mysql` client used the default character set if it automatically reconnected to the server, which is incorrect if the character set had been changed. To enable the character set to remain synchronized on the client and server, the `mysql` command `charset` (or `\C`) that changes the default character set and now also issues a `SET NAMES` statement. The changed character set is used for reconnects. (Bug #11972)
- If a `DROP VIEW` statement named multiple views, it stopped with an error if a nonexistent view was named and did not drop the remaining views. Now it continues on and reports an error at the end, similar to `DROP TABLE`. (Bug #11551)
- The server now issues a warning if it removes leading spaces from an alias. (Bug #10977)
- For a successful dump, `mysqldump` now writes a SQL comment to the end of the dump file in the following format:

```
-- Dump completed on YYYY-MM-DD hh:mm:ss
```

(Bug #10877)

- For spatial data types, the server formerly returned these as `VARSTRING` values with a binary collation. Now the server returns spatial values as `BLOB` values. (Bug #10166)
- A new system variable, `lc_time_names`, specifies the locale that controls the language used to display day and month names and abbreviations. This variable affects the output from the `DATE_FORMAT()`, `DAYNAME()` and `MONTHNAME()` functions. See [MySQL Server Locale Support](#).
- Using `--with-debug` to configure MySQL with debugging support enables you to use the `--debug="d,parser_debug"` option when you start the server. This causes the Bison parser that is used to process SQL statements to dump a parser trace to the server's standard error output. Typically, this output is written to the error log.
- The bundled yaSSL library was upgraded to version 1.3.7.

Bugs Fixed

- **Security Fix:** A stored routine created by one user and then made accessible to a different user using `GRANT EXECUTE` could be executed by that user with the privileges of the routine's definer. (Bug #18630, CVE-2006-4227)

- **Security Fix:** On Linux, and possibly other platforms using case-sensitive file systems, it was possible for a user granted rights on a database to create or access a database whose name differed only from that of the first by the case of one or more letters. (Bug #17647, CVE-2006-4226)
- **MySQL Cluster; Packaging:** The `ndb_mgm` program was included in both the `MySQL-ndb-tools` and `MySQL-ndb-management` RPM packages, resulting in a conflict if both were installed. Now `ndb_mgm` is included only in `MySQL-ndb-tools`. (Bug #21058)
- **MySQL Cluster:** Setting `TransactionDeadlockDetectionTimeout` to a value greater than 12000 would cause scans to deadlock, time out, fail to release scan records, until the cluster ran out of scan records and stopped processing. (Bug #21800)
- **MySQL Cluster:** A memory leak occurred when running `ndb_mgm -e "SHOW"`. (Bug #21670)
- **MySQL Cluster:** The server provided a nondescriptive error message when encountering a fatally corrupted REDO log. (Bug #21615)
- **MySQL Cluster:** A partial rollback could lead to node restart failures. (Bug #21536)
- **MySQL Cluster:** The failure of a unique index read due to an invalid schema version could be handled incorrectly in some cases, leading to unpredictable results. (Bug #21384)
- **MySQL Cluster:** In a cluster with more than 2 replicas, a manual restart of one of the data nodes could fail and cause the other nodes in the same node group to shut down. (Bug #21213)
- **MySQL Cluster:** Some queries involving joins on very large NDB tables could crash the MySQL server. (Bug #21059)
- **MySQL Cluster:** Restarting a data node while DDL operations were in progress on the cluster could cause other data nodes to fail. This could also lead to `mysqld` hanging or crashing under some circumstances. (Bug #21017, Bug #21050)
- **MySQL Cluster:** In some situations with a high disk-load, writing of the redo log could hang, causing a crash with the error message `GCP STOP detected`. (Bug #20904)
- **MySQL Cluster:** When the redo buffer ran out of space, a `Pointer too large` error was raised and the cluster could become unusable until restarted with `--initial`. (Bug #20892)
- **MySQL Cluster:** A vague error message was returned when reading both schema files during a restart of the cluster. (Bug #20860)
- **MySQL Cluster:** Incorrect values were inserted into `AUTO_INCREMENT` columns of tables restored from a cluster backup. (Bug #20820)
- **MySQL Cluster:** When attempting to restart the cluster following a data import, the cluster failed during Phase 4 of the restart with `Error 2334: Job buffer congestion`. (Bug #20774)
- **MySQL Cluster:** `REPLACE` statements did not work correctly on an NDB table having both a primary key and a unique key. In such cases, proper values were not set for columns which were not explicitly referenced in the statement. (Bug #20728)
- **MySQL Cluster:** The server did not honor the value set for `ndb_cache_check_time` in the `my.cnf` file. (Bug #20708)
- **MySQL Cluster:** `ndb_size.pl` and `ndb_error_reporter` were missing from RPM packages. (Bug #20426)
- **MySQL Cluster:** Running `ndbd --nowait-nodes=id` where `id` was the node ID of a node that was already running failed with an invalid error message. (Bug #20419)

- **MySQL Cluster:** A node failure during a scan could sometime cause the node to crash when restarting too quickly following the failure. (Bug #20197)
- **MySQL Cluster:** It was possible to use port numbers greater than 65535 for `ServerPort` in the `config.ini` file. (Bug #19164)
- **MySQL Cluster:** Under certain circumstances, a node that was shut down then restarted could hang during the restart. (Bug #18863)
- **MySQL Cluster:** Trying to create or drop a table while a node was restarting caused the node to crash. This is now handled by raising an error. (Bug #18781)
- **MySQL Cluster:** The server failed with a nondescriptive error message when out of data memory. (Bug #18475)
- **MySQL Cluster:** For `NDB` and possibly `InnoDB` tables, a `BEFORE UPDATE` trigger could insert incorrect values. (Bug #18437)
- **MySQL Cluster:** `SELECT ... FOR UPDATE` failed to lock the selected rows. (Bug #18184)
- **MySQL Cluster:** `pererror` did not properly report `NDB` error codes. (Bug #16561)
- **MySQL Cluster:** A Cluster whose storage nodes were installed from the `MySQL-ndb-storage-*` RPMs could not perform `CREATE` or `ALTER` operations that made use of nondefault character sets or collations. (Bug #14918)
- **MySQL Cluster:** The management client `ALL STATUS` command could sometimes report the status of some data nodes incorrectly. (Bug #13985)
- **MySQL Cluster:** An issue that arose from a patch for Bug #19852 made in MySQL 5.0.23 was corrected. (See [Changes in MySQL 5.0.23 \(Not released\)](#).)

References: This issue is a regression of: Bug #19852.

- **Replication; Cluster Replication:** In some cases, a large number of MySQL servers sending requests to the cluster simultaneously could cause the cluster to crash. This could also be triggered by many `NDB` API clients making simultaneous event subscriptions or unsubscriptions. (Bug #20683)
- **Replication:** `CREATE PROCEDURE`, `CREATE FUNCTION`, `CREATE TRIGGER`, and `CREATE VIEW` statements containing multi-line comments (`/* ... */`) could not be replicated. (Bug #20438)
- **Cluster API:** Invoking the MGM API function `ndb_mgm_listen_event()` caused a memory leak. (Bug #21671)
- **Cluster API:** The MGM API function `ndb_logevent_get_fd()` was not implemented. (Bug #21129)
- **Cluster API:** `NdbScanOperation::readTuples()` and `NdbIndexScanOperation::readTuples()` ignored the `batch` parameter. (Bug #20252)
- Some Linux-x86_64-icc packages (of previous releases) mistakenly contained 32-bit binaries. Only `ICC` builds are affected, not `gcc` builds. Solaris and FreeBSD x86_64 builds are not affected. (Bug #22238)
- Running `SHOW MASTER LOGS` at the same time as binary log files were being switched would cause `mysqld` to hang. (Bug #21965)
- `libmysqlclient` defined a symbol `BN_bin2bn` which belongs to OpenSSL. This could break applications that also linked against OpenSSL's `libcrypto` library. The fix required correcting an error in a build script that was failing to add rename macros for some functions. (Bug #21930)

- `character_set_results` can be `NULL` to signify “no conversion,” but some code did not check for `NULL`, resulting in a server crash. (Bug #21913)
- A `NUL` byte within a prepared statement string caused the rest of the string not to be written to the query log, permitting logging to be bypassed. (Bug #21813)
- `COUNT(*)` queries with `ORDER BY` and `LIMIT` could return the wrong result.



Note

This problem was introduced by the fix for Bug #9676, which limited the rows stored in a temporary table to the `LIMIT` clause. This optimization is not applicable to nongroup queries with aggregate functions. The current fix disables the optimization in such cases.

(Bug #21787)

References: This issue is a regression of: Bug #9676.

- `INSERT ... SELECT` sometimes generated a spurious `Column count doesn't match value count` error. (Bug #21774)
- `EXPORT_SET()` did not accept arguments with coercible character sets. (Bug #21531)
- `mysqldump` incorrectly tried to use `LOCK TABLES` for tables in the `INFORMATION_SCHEMA` database. (Bug #21527)
- Memory overruns could occur for certain kinds of subqueries. (Bug #21477)
- A `DATE` can be represented as an integer (such as `20060101`) or as a string (such as `'2006.01.01'`). When a `DATE` (or `TIME`) column is compared in one `SELECT` against both representations, constant propagation by the optimizer led to comparison of `DATE` as a string against `DATE` as an integer. This could result in integer comparisons such as `2006` against `20060101`, erroneously producing a false result. (Bug #21475)
- Adding `ORDER BY` to a `SELECT DISTINCT(expr)` query could produce incorrect results. (Bug #21456)
- Database and table names have a maximum length of 64 characters (even if they contain multibyte characters), but were truncated to 64 bytes.



Note

This fix was reverted in MySQL 5.0.26.

(Bug #21432)

- With `max_sp_recursion` set to 0, a stored procedure that executed a `SHOW CREATE PROCEDURE` statement for itself triggered a recursion limit exceeded error, though the statement involves no recursion. (Bug #21416)
- On 64-bit Windows, a missing table generated error 1017, not the correct value of 1146. (Bug #21396)
- The optimizer sometimes produced an incorrect row-count estimate after elimination of `const` tables. This resulted in choosing extremely inefficient execution plans in some cases when distribution of data in joins were skewed. (Bug #21390)
- A query result could be sorted improperly when using `ORDER BY` for the second table in a join. (Bug #21302)

- Query results could be incorrect if the `WHERE` clause contained `t.key_part NOT IN (val_list)`, where `val_list` is a list of more than 1000 constants. (Bug #21282)
- For user-defined functions created with `CREATE FUNCTION`, the `DEFINER` clause is not legal, but no error was generated. (Bug #21269)
- The `SELECT` privilege was required for an insert on a view, instead of the `INSERT` privilege. (Bug #21261)
References: This issue is a regression of: Bug #20989.
- Subqueries on `INFORMATION_SCHEMA` tables could erroneously return an empty result. (Bug #21231)
- `mysql_upgrade` created temporary files in a possibly insecure way. (Bug #21224)
- When `DROP DATABASE` or `SHOW OPEN TABLES` was issued while concurrently in another connection issuing `DROP TABLE`, `RENAME TABLE`, `CREATE TABLE LIKE` or any other statement that required a name lock, the server crashed. (Bug #21216, Bug #19403)
- The `--master-data` option for `mysqldump` requires certain privileges, but `mysqldump` generated a truncated dump file without producing an appropriate error message or exit status if the invoking user did not have those privileges. (Bug #21215)
- Some prepared statements caused a server crash when executed a second time. (Bug #21166)
- The optimizer assumed that if `(a=x AND b=x)` is true, `(a=x AND b=x) AND a=b` is also true. But that is not always so if `a` and `b` have different data types. (Bug #21159)
- `SHOW INNODB STATUS` contained some duplicate output. (Bug #21113)
- `InnoDB` was slow with more than 100,000 `.idb` files. (Bug #21112)
- Performing an `INSERT` on a view that was defined using a `SELECT` that specified a collation and a column alias caused the server to crash. (Bug #21086)
- `ALTER VIEW` did not retain existing values of attributes that had been originally specified but were not changed in the `ALTER VIEW` statement. (Bug #21080)
- For `InnoDB` tables, the server could crash when executing `NOT IN(...)` subqueries. (Bug #21077)
- The `myisam_stats_method` variable was mishandled when set from an option file or on the command line. (Bug #21054)
- With `query_cache_type` set to 0, `RESET QUERY CACHE` was very slow and other threads were blocked during the operation. Now a cache reset is faster and nonblocking. (Bug #21051)
- `mysql` crashed for very long arguments to the `connect` command. (Bug #21042)
- A query using `WHERE column = constant OR column IS NULL` did not return consistent results on successive invocations. The `column` in each part of the `WHERE` clause could be either the same column, or two different columns, for the effect to be observed. (Bug #21019)
- Performance during an import on a table with a trigger that called a stored procedure was severely degraded. This issue first arose in MySQL 5.0.18. (Bug #21013)
- A query of the form shown here caused the server to crash:

```
SELECT * FROM t1 NATURAL JOIN (
```

```
t2 JOIN (  
    t3 NATURAL JOIN t4,  
    t5 NATURAL JOIN t6  
)  
ON (t3.id3 = t2.id3 AND t5.id5 = t2.id5)  
);
```

(Bug #21007)

- `STR_TO_DATE()` sometimes would return `NULL` if the `%D` format specifier was not the last specifier in the format string. (Bug #20987)
- A query using `WHERE NOT (column < ANY (subquery))` yielded a different result from the same query using the same `column` and `subquery` with `WHERE (column > ANY (subquery))`. (Bug #20975)
- In debugging mode, `mysqld` printed `server_init` rather than `network_init` during network initialization. (Bug #20968)
- Under certain circumstances, `AVG(key_val)` returned a value but `MAX(key_val)` returned an empty set due to incorrect application of `MIN()/MAX()` optimization. (Bug #20954)
- On Windows, `mysql_upgrade.exe` could not find `mysqlcheck.exe`. (Bug #20950)
- Use of zero-length variable names caused a server crash. (Bug #20908)
- The server crashed when using the range access method to execute a subquery with a `ORDER BY DESC` clause. (Bug #20869)
- For certain queries, the server incorrectly resolved a reference to an aggregate function and crashed. (Bug #20868)
- Using aggregate functions in subqueries yielded incorrect results under certain circumstances due to incorrect application of `MIN()/MAX()` optimization. (Bug #20792)
- If a column definition contained a character set declaration, but a `DEFAULT` value began with an introducer, the introducer character set was used as the column character set. (Bug #20695)
- Multiplication of `DECIMAL` values could produce incorrect fractional part and trailing garbage caused by signed overflow. (Bug #20569)
- Users who had the `SHOW VIEW` privilege for a view and privileges on one of the view's base tables could not see records in `INFORMATION_SCHEMA` tables relating to the base table. (Bug #20543)
- The `MD5()`, `SHA1()`, and `ENCRYPT()` functions should return a binary string, but the result sometimes was converted to the character set of the argument. `MAKE_SET()` and `EXPORT_SET()` now use the correct character set for their default separators, resulting in consistent result strings which can be coerced according to normal character set rules. (Bug #20536)
- A subquery that contained `LIMIT N, 1` could return more than one row. (Bug #20519)
- Creation of a view as a join of views or tables could fail if the views or tables are in different databases. (Bug #20482)
- `SELECT` statements using `GROUP BY` against a view could have missing columns in the output when there was a trigger defined on one of the base tables for the view. (Bug #20466)
- For connections that required a `SUBJECT` value, a check was performed to verify that the value was correct, but the connection was not refused if not. (Bug #20411)

- Some user-level errors were being written to the server's error log, which is for server errors. (Bug #20402)
- `perror` crashed on Solaris due to `NULL` return value of `strerror()` system call. (Bug #20145)
- For `mysql` , escaping with backslash sometimes did not work. (Bug #20103)
- Use of `MIN()` or `MAX()` with `GROUP BY` on a `ucs2` column could cause a server crash. (Bug #20076)
- `mysqld --flush` failed to flush `MyISAM` table changes to disk following an `UPDATE` statement for which no updated column had an index. (Bug #20060)
- A user-defined function that is called on each row of a returned result set, could receive an `in_null` state that is set, if it was set previously. Now, the `is_null` state is reset to false before each invocation of a UDF. (Bug #19904)
- The `query` command for `mysqltest` did not work. (Bug #19890)
- When executing a `SELECT` with `ORDER BY` on a view that is constructed from a `SELECT` statement containing a stored function, the stored function was evaluated too many times. (Bug #19862)
- The first time a user who had been granted the `CREATE ROUTINE` privilege used that privilege to create a stored procedure or function, the `Password` column in that user's row in the `mysql.user` table was set to `NULL` . (Bug #19857)
- For `TIME_FORMAT()` , the `%H` and `%k` format specifiers can return values larger than two digits (if the hour is greater than 99), but for some query results that contained three-character hours, column values were truncated. (Bug #19844)
- Using `SELECT` on a corrupt `MyISAM` table using the dynamic record format could cause a server crash. (Bug #19835)
- Using cursors with `READ COMMITTED` isolation level could cause `InnoDB` to crash. (Bug #19834)
- The `yaSSL` library bundled with `libmysqlclient` had some conflicts with `OpenSSL` . Now macros are used to rename the conflicting symbols to have a prefix of `ya` . (Bug #19810)
- On 64-bit systems, use of the `cp1250` character set with a primary key column in a `LIKE` clause caused a server crash for patterns having letters in the range 128..255. (Bug #19741)
- `DESCRIBE` returned the type `BIGINT` for a column of a view if the column was specified by an expression over values of the type `INT` . (Bug #19714)
- An issue with `yaSSL` prevented `Connector/J` clients from connecting to the server using a certificate. (Bug #19705)
- A cast problem caused incorrect results for prepared statements that returned float values when `MySQL` was compiled with `gcc 4.0` . (Bug #19694)
- The `mysql_list_fields()` C API function returned the incorrect table name for views. (Bug #19671)
- If a query had a condition of the form `tableX.key = tableY.key` , which participated in equality propagation and also was used for `ref` access, then early `ref-access NULL` filtering was not performed for the condition. This could make query execution slower. (Bug #19649)
- Repeated `DROP TABLE` statements in a stored procedure could sometimes cause the server to crash. (Bug #19399)
- When not running in strict mode, the server failed to convert the invalid years portion of a `DATE` or `DATETIME` value to `'0000'` when inserting it into a table.

**Note**

This fix was reverted in MySQL 5.0.40.

(Bug #19370)

References: See also: Bug #25301.

- The final parenthesis of a `CREATE INDEX` statement occurring in a stored procedure was omitted from the binary log when the stored procedure was called. (Bug #19207)
- A `SELECT` with a subquery that was bound to the outer query over multiple columns returned different results when a constant was used instead of one of the dependant columns. (Bug #18925)
- Setting `myisam_repair_threads` caused any repair operation on a `MyISAM` table to fail to update the cardinality of indexes, instead making them always equal to 1. (Bug #18874)
- `FEDERATED` tables raised invalid duplicate key errors when attempting on one server to insert rows having the same primary key values as rows that had been deleted from the linked table on the other server. (Bug #18764)
- The implementation for `UNCOMPRESS()` did not indicate that it could return `NULL`, causing the optimizer to do the wrong thing. (Bug #18539)
- Using `> ALL` with subqueries that return no rows yielded incorrect results under certain circumstances due to incorrect application of `MIN()/MAX()` optimization. (Bug #18503)
- Referring to a stored function qualified with the name of one database and tables in another database caused a “table doesn't exist” error. (Bug #18444)
- Triggers on tables in the `mysql` database caused a server crash. Triggers for tables in this database are no longer permitted. (Bug #18361, Bug #18005)
- The length of the pattern string prefix for `LIKE` operations was calculated incorrectly for multibyte character sets. As a result, the scanned range was wider than necessary if the prefix contained any multibyte characters, and rows could be missing from the result set. (Bug #18359, Bug #16674)
- Multiple invocations of the `REVERSE()` function could return different results. (Bug #18243)
- The optimizer did not take advantage of indexes on columns used for the second or third arguments of `BETWEEN`. (Bug #18165)
- For table-format output, `mysql` did not always calculate columns widths correctly for columns containing multibyte characters in the column name or contents. (Bug #17939)
- The character set was not being properly initialized for `CAST()` with a type such as `CHAR(2) BINARY`, which resulted in incorrect results or a server crash. (Bug #17903)
- Checking a `MyISAM` table (using `CHECK TABLE`) having a spatial index and only one row would wrongly indicate that the table was corrupted. (Bug #17877)
- A stored procedure that created and invoked a prepared statement was not executed when called in a `mysqld` init-file. (Bug #17843)
- It is possible to create `MERGE` tables into which data cannot be inserted (by not specifying a `UNION` clause. However, when an insert was attempted, the error message was confusing. Now an error occurs indicating that the table is read only. (Bug #17766)

- Attempting to insert a string of greater than 4096 bytes into a `FEDERATED` table resulted in the error `ERROR 1296 (HY000) at line 2: Got error 10000 'Error on remote system: 1054: Unknown column 'string-value' from FEDERATED`. This error was raised regardless of the type of column involved (`VARCHAR`, `TEXT`, and so on.) (Bug #17608)
- Views could not be updated within a stored function or trigger. (Bug #17591)
- Use of the `--prompt` option or `prompt` command caused `mysql` to be unable to connect to the Instance Manager. (Bug #17485)
- `N'xxx'` and `_utf8'xxx'` were not treated as equivalent because `N'xxx'` failed to unescape backslashes (`\`) and doubled apostrophe/single quote characters (`' '`). (Bug #17313)
- Use of the join cache in favor of an index for `ORDER BY` operations could cause incorrect result sorting. (Bug #17212)
- The `PASSWORD()` function returned invalid results when used in some `UNION` queries. (Bug #16881)
- `ORDER BY RAND() LIMIT 1` always set a user variable to the last possible value from the table. (Bug #16861)
- When performing a `GROUP_CONCAT()`, the server transformed `BLOB` columns `VARCHAR` columns, which could cause erroneous results when using Connector/J and possibly other MySQL APIs. (Bug #16712)
- Stored procedures did not use the character set defined for the database in which they were created. (Bug #16676)
- Some server errors were not reported to the client, causing both to try to read from the connection until a hang or crash resulted. (Bug #16581)
- On Windows, a definition for `mysql_set_server_option()` was missing from the C client library. (Bug #16513)
- Updating a column of a `FEDERATED` table to `NULL` sometimes failed. (Bug #16494)
- For `SELECT ... FOR UPDATE` statements that used `DISTINCT` or `GROUP BY` over all key parts of a unique index (or primary key), the optimizer unnecessarily created a temporary table, thus losing the linkage to the underlying unique index values. This caused a `Result set not updatable` error. (The temporary table is unnecessary because under these circumstances the distinct or grouped columns must also be unique.) (Bug #16458)
- Using `ANY` with “nontable” subqueries such as `SELECT 1` yielded incorrect results under certain circumstances due to incorrect application of `MIN()`/`MAX()` optimization. (Bug #16302)
- A subquery in the `WHERE` clause of the outer query and using `IN` and `GROUP BY` returned an incorrect result. (Bug #16255)
- A query could produce different results with and without an index, if the `WHERE` clause contained a range condition that used an invalid `DATETIME` constant. (Bug #16249)
- `TIMESTAMPDIFF()` examined only the date and ignored the time when the requested difference unit was months or quarters. (Bug #16226)
- Using tables from MySQL 4.x in MySQL 5.x, in particular those with `VARCHAR` fields and using `INSERT DELAYED` to update data in the table would result in either data corruption or a server crash. (Bug #16218, Bug #17294, Bug #16611)
- The value returned by a stored function returning a string value was not of the declared character set. (Bug #16211)

- The `index_merge/Intersection` optimizer could experience a memory overrun when the number of table columns covered by an index was sufficiently large, possibly resulting in a server crash. (Bug #16201)
- `DECIMAL` columns were handled incorrectly in two respects :
 1. When the precision of the column was too small for the value. In this case, the original value was returned instead of an error.
 2. When the scale of the column was set to 0. In this case, the value. In this case, the value was treated as though the scale had been defined as 2.

(Bug #16172)

- Certain queries having a `WHERE` clause that included conditions on multi-part keys with more than 2 key parts could produce incorrect results and send `[Note] Use_count: Wrong count for key at...` messages to `STDERR`. (Bug #16168)
- When a row was inserted through a view but did not specify a value for a column that had no default value in the base table, no warning or error occurred. Now a warning occurs, or an error in strict SQL mode. (Bug #16110)
- When `NOW()` was used in a `BETWEEN` clause of the definition for a view, it was replaced with a constant in the view. (Bug #15950)
- The C API failed to return a status message when invoking a stored procedure. (Bug #15752)
- `mysqlimport` sends a `set @@character_set_database=binary` statement to the server, but this is not understood by pre-4.1 servers. Now `mysqlimport` encloses the statement within a `/*!40101 ... */` comment so that old servers will ignore it. (Bug #15690)
- For the `CSV` storage engine, memory-mapped pages of the data file were not invalidated when new data was appended to the file using traditional (file descriptor-based) I/O primitives. (Bug #15669)
- `SHOW GRANTS FOR CURRENT_USER` did not return definer grants when executed in `DEFINER` context (such as within a stored procedure defined with `SQL SECURITY DEFINER`), it returned the invoker grants. (Bug #15298)
- The `--collation-server` server option was being ignored. With the fix, if you choose a nondefault character set with `--character-set-server`, you should also use `--collation-server` to specify the collation. (Bug #15276)
- The server crashed if it tried to access a `CSV` table for which the data file had been removed. (Bug #15205)
- Tables created with the `FEDERATED` storage engine did not permit indexes using `NULL` columns. (Bug #15133)
- When using tables containing `VARCHAR` columns created under MySQL 4.1 with a 5.0 or later server, for some queries the metadata sent to the client could have an empty column name. (Bug #14897)
- `CREATE TABLE ... SELECT` statements that selected `GEOMETRY` values resulted in a table that contained `BLOB` columns, not `GEOMETRY` columns. (Bug #14807)
- When setting a column to its implicit default value as the result of inserting a `NULL` into a `NOT NULL` column as part of a multi-row insert or `LOAD DATA` operation, the server returned a misleading warning message. (Bug #14770)

- The use of `WHERE col_name IS NULL` in `SELECT` statements reset the value of `LAST_INSERT_ID()` to zero. (Bug #14553)
- Inserts into `BIT` columns of `FEDERATED` tables did not work. (Bug #14532)
- Using `SELECT` and a table join while running a concurrent `INSERT` operation would join incorrect rows. (Bug #14400)
- Prepared statements caused general log and server memory corruption. (Bug #14346)
- `libmysqld` produced some warnings to `stderr` which could not be silenced. These warnings now are suppressed. (Bug #13717)
- The Instance Manager permitted `STOP INSTANCE` to be used on a server instance that was not running. (Bug #12673)
- For very complex `SELECT` statements could create temporary tables that were too large, and for which the temporary files were not removed, causing subsequent queries to fail. (Bug #11824)
- `USE` did not refresh database privileges when employed to re-select the current database. (Bug #10979)
- The type of the value returned by the `VARIANCE()` function varied according to the type of the input value. The function should always return a `DOUBLE` value. (Bug #10966)
- The same trigger error message was produced under two conditions: The trigger duplicated an existing trigger name, or the trigger duplicated an existing combination of action and event. Now different messages are produced for the two conditions so as to be more informative. (Bug #10946)
- `CREATE USER` did not respect the 16-character user name limit. (Bug #10668)
- A server or network failure with an open client connection would cause the client to hang even though the server was no longer available.

As a result of this change, the `MYSQL_OPT_READ_TIMEOUT` and `MYSQL_OPT_WRITE_TIMEOUT` options for `mysql_options()` now apply to TCP/IP connections on all platforms. Previously, they applied only to Windows. (Bug #9678)

- `INSERT INTO ... SELECT ... LIMIT 1` could be slow because the `LIMIT` was ignored when selecting candidate rows. (Bug #9676)
- The optimizer could produce an incorrect result after `AND` with collations such as `latin1_german2_ci`, `utf8_czech_ci`, and `utf8_lithuanian_ci`. (Bug #9509)
- A stored procedure with a `CONTINUE` handler that encountered an error continued to execute a statement that caused an error, rather with the next statement following the one that caused the error. (Bug #8153)
- For ODBC compatibility, MySQL supports use of `WHERE col_name IS NULL` for `DATE` or `DATETIME` columns that are `NOT NULL`, to permit column values of `'0000-00-00'` or `'0000-00-00 00:00:00'` to be selected. However, this was not working for `WHERE` clauses in `DELETE` statements. (Bug #8143)
- A user variable set to a value selected from an unsigned column was stored as a signed value. (Bug #7498)
- The `--with-collation` option was not honored for client connections. (Bug #7192)

Changes in MySQL 5.0.24a (2006-08-25)

This is a bugfix release for the current production release family. It replaces MySQL 5.0.24.

Bugs Fixed

- The shared compatibility RPM files were missing some files. (Bug #22251)
- `mysqld` could crash when closing temporary tables. (Bug #21582)
- MySQL 5.0.24 introduced an ABI incompatibility, which this release reverts. Programs compiled against 5.0.24 are not compatible with any other version and must be recompiled. (Bug #21543)
- Path name separator and device characters were not correctly parameterized for NetWare, causing `mysqld` startup errors. (Bug #21537)
- Closing of temporary tables failed if binary logging was not enabled. (Bug #20919)
- For statements that have a `DEFINER` clause such as `CREATE TRIGGER` or `CREATE VIEW`, long user names or host names could cause a buffer overflow. (Bug #16899)

Changes in MySQL 5.0.24 (2006-07-27)

This is a bugfix release for the current production release family.

This section documents all changes and bug fixes that have been applied since the last official MySQL release. If you would like to receive more fine-grained and personalized *update alerts* about fixes that are relevant to the version and features you use, please consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details, please see (<http://www.mysql.com/products/enterprise>).

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- In the `INFORMATION_SCHEMA.ROUTINES` table the `ROUTINE_DEFINITION` column now is defined as `NULL` rather than `NOT NULL`. Also, `NULL` rather than the empty string is returned as the column value if the user does not have sufficient privileges to see the routine definition. (Bug #20230)
- The `LEFT()` and `RIGHT()` functions return `NULL` if any argument is `NULL`. (Bug #11728)
- The `innodb_log_arch_dir` system variable (which has been unused since MySQL 4.0.6) is now deprecated and should no longer be used. It will be removed in MySQL 5.1.
- Program Database (PDB) files (with file name extension `.pdb`) are now included by default in Windows distributions. These can be used to help diagnose problems with `mysqld` and other tools. See [Debugging a MySQL Server](#).

Bugs Fixed

- **Security Fix:** If a user has access to `MyISAM` table `t`, that user can create a `MERGE` table `m` that accesses `t`. However, if the user's privileges on `t` are subsequently revoked, the user can continue to access `t` by doing so through `m`. If this behavior is undesirable, you can start the server with the new `--skip-merge` option to disable the `MERGE` storage engine. (Bug #15195, CVE-2006-4031)
- **MySQL Cluster:** The `ndb_size.pl` script did not account for `TEXT` and `BLOB` column values correctly. (Bug #21204)
- **MySQL Cluster:** The repeated creating and dropping of a table would eventually lead to `NDB Error 826, Too many tables and attributes ... Insufficient space`. (Bug #20847)

- **Replication:** A race condition during slave server shutdown caused an assert failure. (Bug #20850)
- **Replication:** With the `auto_increment_increment` system variable set larger than 1, if the next generated `AUTO_INCREMENT` value would be larger than the column's maximum value, the value would be clipped down to that maximum value and inserted, even if the resulting value would not be in the generated sequence. This could cause problems for master-master replication. Now the server clips the value down to the previous value in the sequence, which correctly produces a duplicate-key error if that value already exists in the column. (Bug #20524)
- **Replication:** If a table on a slave server had a higher `AUTO_INCREMENT` counter than the corresponding master table (even though all rows of the two tables were identical), in some cases `REPLACE` or `INSERT ... ON DUPLICATE KEY UPDATE` would not replicate properly using statement-based logging. (Different values would be inserted on the master and slave.) (Bug #20188)
- Under heavy load (executing more than 1024 simultaneous complex queries), a problem in the code that handles internal temporary tables could lead to writing beyond allocated space and memory corruption.

Use of more than 1024 simultaneous cursors server wide also could lead to memory corruption. This applies to both stored procedure cursors and C API cursors. (Bug #21206)
- Failure to account for a `NULL` table pointer on big-endian machines could cause a server crash during type conversion. (Bug #21135)
- `mysqldump` sometimes did not select the correct database before trying to dump views from it, resulting in an empty result set that caused `mysqldump` to die with a segmentation fault. (Bug #21014)
- A `SELECT` that used a subquery in the `FROM` clause that did not select from a table failed when the subquery was used in a join. (Bug #21002)
- `REPLACE ... SELECT` for a view required the `INSERT` privilege for tables other than the table being modified. (Bug #20989)
- Issuing a `SHOW CREATE FUNCTION` or `SHOW CREATE PROCEDURE` statement without sufficient privileges could crash the `mysql` client. (Bug #20664)
- In a view defined with `SQL SECURITY DEFINER`, the `CURRENT_USER()` function returned the invoker, not the definer. (Bug #20570)
- `SELECT @@INSERT_ID` displayed a value unrelated to a preceding `SET INSERT_ID`. (It returned `LAST_INSERT_ID` instead.) (Bug #20392)
- The `mysql` client did not understand `help` commands that had spaces at the end. (Bug #20328)
- `mysqldump` produced a malformed dump file when dumping multiple databases that contained views. (Bug #20221)
- For a `DATE` parameter sent using a `MYSQL_TIME` data structure, `mysql_stmt_execute()` zeroed the hour, minute, and second members of the structure rather than treating them as read only. (Bug #20152)
- Performing `INSERT ... SELECT ... JOIN ... USING` without qualifying the column names caused `ERROR 1052 "column 'x' in field list is ambiguous"` even in cases where the column references were unambiguous. (Bug #18080)
- Using the extended syntax for `TRIM()`—that is, `TRIM(... FROM ...)`—in a `SELECT` statement defining a view caused an invalid syntax error when selecting from the view. (Bug #17526)
- Assignments of values to variables of type `TEXT` were handled incorrectly in stored routines. (Bug #17225)

- `DATE_ADD()` and `DATE_SUB()` returned `NULL` when the result date was on the day '9999-12-31'. (Bug #12356)
- The `DATA DIRECTORY` table option did not work for `TEMPORARY` tables. (Bug #8706)
- Bug #10952 may cause inadvertent data loss. A fix for this bug was included in MySQL 5.0.23, but the approach used caused a loss of intended functionality. Because of this, that fix has been reverted in MySQL 5.0.24. As a consequence, the risk of inadvertent data loss still exists (see Bug #10952).

References: Reverted patches: Bug #10952.

Changes in MySQL 5.0.23 (Not released)

MySQL 5.0.23 was never officially released.

This section documents all changes and bug fixes that have been applied since the last official MySQL release. If you would like to receive more fine-grained and personalized *update alerts* about fixes that are relevant to the version and features you use, please consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details, please see (<http://www.mysql.com/products/enterprise>).

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- **Incompatible Change:** For `GRANT` and `REVOKE`, `ON *` previously granted and revoked privileges for the default database if there was a default database and global privileges if there was none. Now `ON *` requires a default database and produces an error if there is none.
- **Important Change; MySQL Cluster:** The status variables `Ndb_connected_host` and `Ndb_connected_port` were renamed to `Ndb_config_from_host` and `Ndb_config_from_port`, respectively.
- **MySQL Cluster:** The limit of 2048 ordered indexes per cluster has been lifted. There is now no upper limit on the number of ordered indexes (including `AUTO_INCREMENT` columns) that may be used. (Bug #14509)
- The `mysqldumpslow` script has been moved from client RPM packages to server RPM packages. This corrects a problem where `mysqldumpslow` could not be used with a client-only RPM install, because it depends on `my_print_defaults` which is in the server RPM. (Bug #20216)
- Added the `log_queries_not_using_indexes` system variable. (Bug #19616)
- Added the `ssl_ca`, `ssl_capath`, `ssl_cert`, `ssl_cipher`, and `ssl_key` system variables, which display the values given using the corresponding command options. See [Command Options for Secure Connections](#). (Bug #19606)
- SQL syntax for prepared statements now supports `ANALYZE TABLE`, `OPTIMIZE TABLE`, and `REPAIR TABLE`. (Bug #19308)
- For a table with an `AUTO_INCREMENT` column, `SHOW CREATE TABLE` now shows the next `AUTO_INCREMENT` value to be generated. (Bug #19025)
- The `ONLY_FULL_GROUP_BY` SQL mode now also applies to the `HAVING` clause. That is, columns not named in the `GROUP BY` clause cannot be used in the `HAVING` clause if not used in an aggregate function. (Bug #18739)

- Added the `--set-charset` option to `mysqlbinlog` to enable the character set to be specified for processing binary log files. (Bug #18351)
- The bundled yaSSL library was upgraded to version 1.3.5. This improves handling of certain problems with SSL-related command options. (Bug #17737)
- Added the `--ssl-verify-server-cert` option to MySQL client programs. This option causes the server's Common Name value in its certificate to be verified against the host name used when connecting to the server, and the connection is rejected if there is a mismatch. Added `MYSQL_OPT_SSL_VERIFY_SERVER_CERT` option for the `mysql_options()` C API function to enable this verification. This feature can be used to prevent man-in-the-middle attacks. Verification is disabled by default. (Bug #17208)
- It is now possible to use `NEW.var_name` values within triggers as `INOUT` parameters to stored procedures. (Bug #14635)
- Added the `--angel-pid-file` option to `mysqlmanager` for specifying the file in which the angel process records its process ID when `mysqlmanager` runs in daemon mode. (Bug #14106)
- The `mysql_get_ssl_cipher()` C API function was added.
- The `mysql_upgrade` command has been converted from a shell script to a C program, so it is available on non-Unix systems such as Windows. This program should be run for each MySQL upgrade. See [mysql_upgrade — Check Tables for MySQL Upgrade](#).
- Binary distributions that include SSL support now are built using yaSSL when possible.

Bugs Fixed

- **Security Fix:** A `NUL` byte within a comment in a statement string caused the rest of the string not to be written to the query log, permitting logging to be bypassed. (Bug #17667, CVE-2006-0903)
- **MySQL Cluster:** The `ndb_mgm` client command `ALL CLUSTERLOG STATISTICS=15` had no effect. (Bug #20336)
- **MySQL Cluster:** The failure of a data node when preparing to commit a transaction (that is, while the node's status was `CS_PREPARE_TO_COMMIT`) could cause the failure of other cluster data nodes. (Bug #20185)
- **MySQL Cluster:** An internal formatting error caused some management client error messages to be unreadable. (Bug #20016)
- **MySQL Cluster:** Renaming a table in such a way as to move it to a different database failed to move the table's indexes. (Bug #19967)
- **MySQL Cluster:** Running management client commands while `mgmd` was in the process of disconnecting could cause the management server to fail. (Bug #19932)
- **MySQL Cluster:** Running `ALL START` in the `NDB` management client or restarting multiple nodes simultaneously could under some circumstances cause the cluster to crash. (Bug #19930)
- **MySQL Cluster:** `TEXT` columns in Cluster tables having both an explicit primary key and a unique key were not correctly updated by `REPLACE` statements. (Bug #19906)
- **MySQL Cluster:** The cluster's data nodes failed while trying to load data when `NoOfFrangmentLogFiles` was set equal to 1. (Bug #19894)
- **MySQL Cluster:** Restoring a backup with `ndb_restore` failed when the backup had been taken from a cluster whose `DataMemory` had been completely used up. (Bug #19852)

- **MySQL Cluster:** Resources for unique indexes on Cluster table columns were incorrectly allocated, so that only one-fourth as many unique indexes as indicated by the value of `UniqueHashIndexes` could be created. (Bug #19623)
- **MySQL Cluster:** `LOAD DATA LOCAL` failed to ignore duplicate keys in Cluster tables. (Bug #19496)
- **MySQL Cluster:** For `ndb_mgmd`, Valgrind revealed problems with a memory leak and a dependency on an uninitialized variable. (Bug #19318, Bug #20333)
- **MySQL Cluster:** A problem with error handling when `ndb_use_exact_count` was enabled could lead to incorrect values returned from queries using `COUNT()`. A warning is now returned in such cases. (Bug #19202)
- **MySQL Cluster:** `TRUNCATE TABLE` failed on tables having `BLOB` or `TEXT` columns with the error `Lock wait timeout exceeded`. (Bug #19201)
- **MySQL Cluster:** `mysql-test-run.pl` started `NDB` even for test cases that did not need it. (Bug #19083)
- **MySQL Cluster:** Stopping multiple nodes could cause node failure handling not to be completed. (Bug #19039)
- **MySQL Cluster:** The management client `ALL STOP` command shut down `mgmd` processes (as well as `ndbd` processes). (Bug #18966)
- **MySQL Cluster:** `TRUNCATE TABLE` failed to reset the `AUTO_INCREMENT` counter. (Bug #18864)
- **MySQL Cluster:** Repeated `CREATE - INSERT - DROP` operations on tables could in some circumstances cause the MySQL table definition cache to become corrupt, so that some `mysqld` processes could access table information but others could not. (Bug #18595)
- **MySQL Cluster:** Repeated use of the `SHOW` and `ALL STATUS` commands in the `ndb_mgm` client could cause the `mgmd` process to crash. (Bug #18591)
- **MySQL Cluster:** `ndbd` sometimes failed to start with the error `Node failure handling not completed` following a graceful restart. (Bug #18550)
- **MySQL Cluster:** Backups could fail for large clusters with many tables, where the number of tables approached `MaxNoOfTables`. (Bug #17607)
- **MySQL Cluster:** An issue with `ndb_mgmd` prevented more than 27 `mysqld` processes from connecting to a single cluster at one time. (Bug #17150)
- **MySQL Cluster:** Using “stale” `mysqld .frm` files could cause a newly restored cluster to fail. This situation could arise when restarting a MySQL Cluster using the `--initial` option while leaving connected `mysqld` processes running. (Bug #16875)
- **MySQL Cluster:** Data node failures could cause excessive CPU usage by `ndb_mgmd`. (Bug #13987)
- **MySQL Cluster:** Cluster system status variables were not updated properly. (Bug #11459)
- **MySQL Cluster:** Some queries having a `WHERE` clause of the form `c1=val1 OR c2 LIKE 'val2'` were not evaluated correctly. (Bug #17421)
- **MySQL Cluster:** (NDBAPI): Update operations on blobs were not checked for illegal operations.

**Note**

Read locks with blob update operations are now upgraded from read committed to read shared.

- **Replication:** Valgrind revealed an issue with `mysqld` that was corrected: memory corruption in replication slaves when switching databases. (Bug #19022)
- **Replication:** The binary log would create an incorrect `DROP` query when creating temporary tables during replication. (Bug #17263)
- **Replication:** An invalid `GRANT` statement for which `Ok` was returned on a replication master caused an error on the slave and replication to fail. (Bug #6774)
- **Cluster API:** On big-endian platforms, `NdbOperation::write_attr()` did not update 32-bit fields correctly. (Bug #19537)
- A buffer overwrite error in Instance Manager caused a crash. (Bug #20622)
- On Windows, temporary tables containing “:” in the name could not be created. (Bug #20616)
- Valgrind revealed several issues with `mysqld` that were corrected: A dangling stack pointer being overwritten; possible uninitialized data in a string comparison; `syscall()` write parameter pointing to an uninitialized byte. (Bug #20579, Bug #20769, Bug #20783, Bug #20791)
- The `fill_help_tables.sql` file did not contain a `SET NAMES 'utf8'` statement to indicate its encoding. This caused problems for some settings of the MySQL character set such as `big5`. (Bug #20551)
- The `fill_help_tables.sql` file did not load properly if the `ANSI_QUOTES` SQL mode was enabled. (Bug #20542)
- `mysql_upgrade` was missing from binary MySQL distributions. (Bug #20403, Bug #18516, Bug #20556)
- Several aspects of view privileges were being checked incorrectly. (Bug #20363, Bug #18681)
- Queries using an indexed column as the argument for the `MIN()` and `MAX()` functions following an `ALTER TABLE .. DISABLE KEYS` statement returned `Got error 124 from storage engine` until `ALTER TABLE ... ENABLE KEYS` was run on the table. (Bug #20357)
- The thread for `INSERT DELAYED` rows was maintaining a separate `AUTO_INCREMENT` counter, resulting in incorrect values being assigned if `DELAYED` and non-`DELAYED` inserts were mixed. (Bug #20195)
- On Linux, `libmysqlclient` when compiled with yaSSL using the `icc` compiler had a spurious dependency on C++ libraries. (Bug #20119)
- A number of dependency issues in the RPM `bench` and `test` packages caused installation of these packages to fail. (Bug #20078)
- A compatibility issue with NPTL (Native POSIX Thread Library) on Linux could result in a deadlock with `FLUSH TABLES WITH READ LOCK` under some conditions. (Bug #20048)
- Some outer joins were incorrectly converted to inner joins. (Bug #19816)
References: This issue is a regression of: Bug #17146.
- `CREATE DATABASE`, `RENAME DATABASE`, and `DROP DATABASE` could deadlock in cases where there was a global read lock. (Bug #19815)
- The `WITH CHECK OPTION` was not enforced when a `REPLACE` statement was executed against a view. (Bug #19789)
- Multiple-table updates with `FEDERATED` tables could cause a server crash. (Bug #19773)

- `InnoDB` unlocked its data directory before committing a transaction, potentially resulting in nonrecoverable tables if a server crash occurred before the commit. (Bug #19727)
- Subqueries that produced a `BIGINT UNSIGNED` value were being treated as returning a signed value. (Bug #19700)
- `GROUP BY` on an expression that contained a cast to `DECIMAL` produced an incorrect result. (Bug #19667)
- `MERGE` tables did not work reliably with `BIT` columns. (Bug #19648)
- Re-execution of a prepared multiple-table `DELETE` statement that involves a trigger or stored function can result in a server crash. (Bug #19634)
- The range operator failed and caused a server crash for clauses of the form `tbl_name.unsigned_keypart NOT IN (negative_const, ...)`. (Bug #19618)
- `CHECK TABLE` on a `MyISAM` table briefly cleared its `AUTO_INCREMENT` value, while holding only a read lock. Concurrent inserts to that table could use the wrong `AUTO_INCREMENT` value. `CHECK TABLE` no longer modifies the `AUTO_INCREMENT` value. (Bug #19604)
- Using `CONCAT(@user_var, col_name)`, where `col_name` is a column in an `INFORMATION_SCHEMA` table, could cause erroneous duplication of data in the query result. (Bug #19599)
- Some `yaSSL` public function names conflicted with those from `OpenSSL`, causing conflicts for applications that linked against both `OpenSSL` and a version of `libmysqlclient` that was built with `yaSSL` support. The `yaSSL` public functions now are renamed to avoid this conflict. (Bug #19575)
- A view definition that referred to an alias in the `HAVING` clause could be saved in the `.frm` file with the alias replaced by the expression that it referred to, causing failure of subsequent `SELECT * FROM view_name` statements. (Bug #19573)
- `mysql` displayed `NULL` for strings that are empty or contain only spaces. (Bug #19564)
- `InnoDB` failed to increment the `handler_read_prev` counter. (Bug #19542)
- Selecting from a view that used `GROUP BY` on a nonconstant temporal interval (such as `DATE(col) + INTERVAL TIME_TO_SEC(col) SECOND`) could cause a server crash. (Bug #19490)
- `mysqldump` did not dump the table name correctly for some table identifiers that contained unusual characters such as ":". (Bug #19479)
- On 64-bit Windows systems, `REGEXP` for regular expressions with exactly 31 characters did not work. (Bug #19407)
- An outer join of two views that was written using `{ OJ ... }` syntax could cause a server crash. (Bug #19396)
- Race conditions on certain platforms could cause the Instance Manager to fail to initialize. (Bug #19391)
- Use of the `--no-pager` option caused `mysql` to crash. (Bug #19363)
- In the `INFORMATION_SCHEMA.COLUMNS` table, the values for the `CHARACTER_MAXIMUM_LENGTH` and `CHARACTER_OCTET_LENGTH` columns were incorrect for multibyte character sets. (Bug #19236)
- Multiple-table `DELETE` statements containing a subquery that selected from one of the tables being modified caused a server crash. (Bug #19225)
- On Windows, removal of binary log files failed if the files were already open. (Bug #19208)

- Flushing the compression buffer (via `FLUSH TABLE`) no longer increases the size of an unmodified `ARCHIVE` table. (Bug #19204)
- An `ALTER TABLE` operation that does not need to copy data, when executed on a table created prior to MySQL 4.0.25, could result in a server crash for subsequent accesses to the table. (Bug #19192)
- SSL connections using yaSSL on OpenBSD could fail. (Bug #19191)
- Attempting to set the default value of an `ENUM` or `SET` column to `NULL` caused a server crash. (Bug #19145)
- Use of uninitialized user variables in a subquery in the `FROM` clause resulted in invalid entries in the binary log. (Bug #19136)
- A `CREATE TABLE` statement that created a table from a materialized view did not inherit default values from the underlying table. (Bug #19089)
- Index prefixes for `utf8 VARCHAR` columns did not work for `UPDATE` statements. (Bug #19080)
- Premature optimization of nested subqueries in the `FROM` clause that refer to aggregate functions could lead to incorrect results. (Bug #19077)
- The parser leaked memory when its stack needed to be extended. (Bug #18930)
- `BIT` columns in a table could cause joins that use the table to fail. (Bug #18895)
- The MySQL server startup script `/etc/init.d/mysql` (created from `mysql.server`) is now marked to ensure that the system services `ypbind`, `nscd`, `ldap`, and `NTP` are started first (if these are configured on the machine). (Bug #18810)
- The `COM_STATISTICS` command was changed in 5.0.3 to display session status variable values rather than global values. This causes `mysqladmin status` information not to be useful for the `Slow queries` and `Opens` values. Now `COM_STATISTICS` displays the global values for `Slow queries` and `Opens`. (Bug #18669)
- `LOAD DATA FROM MASTER` failed when trying to load the `INFORMATION_SCHEMA` database from the master, because the `INFORMATION_SCHEMA` system database would already exist on the slave. (Bug #18607)
- `BLOB` or `TEXT` arguments to or values returned from stored functions were not copied properly if too long and could become garbled. (Bug #18587)
- The `IN-to-EXISTS` transformation was making a reference to a parse tree fragment that was left out of the parse tree. This caused problems with prepared statements. (Bug #18492)
- `mysqldump` produced garbled output for view definitions. (Bug #18462)
- The configuration information for building the embedded server on Windows was missing a file. (Bug #18455)
- In `mysqltest`, `--sleep=0` had no effect. Now it correctly causes `sleep` commands in test case files to sleep for 0 seconds. (Bug #18312)
- `INFORMATION_SCHEMA.TABLES` provided inconsistent info about invalid views. This could cause server crashes or result in incorrect data being returned for queries that attempt to obtain information from `INFORMATION_SCHEMA` tables about views using stored functions. (Bug #18282)
- On Windows, corrected a crash stemming from differences in Visual C runtime library routines from POSIX behavior regarding invalid file descriptors. (Bug #18275)

- On Windows, terminating `mysqld` with **Control+C** could result in a crash during shutdown. (Bug #18235)
- Selecting data from a `MEMORY` table with a `VARCHAR` column and a `HASH` index over it returned only the first row matched. (Bug #18233)
- The use of `MIN()` and `MAX()` on columns with an index prefix produced incorrect results in some queries. (Bug #18206)
- An entry in the `mysql.proc` table with an empty routine name caused access to the `INFORMATION_SCHEMA.ROUTINES` table to crash the server. (Bug #18177)
- A `UNION` over more than 128 `SELECT` statements that use an aggregate function failed. (Bug #18175)
- Updates to a `MEMORY` table caused the size of `BTREE` indexes for the table to increase. (Bug #18160)
- `SELECT DISTINCT` queries sometimes returned only the last row. (Bug #18068)
- Returning the value of a system variable from a stored function caused a server crash. (Bug #18037)
- An update that used a join of a table to itself and modified the table on both sides of the join reported the table as crashed. (Bug #18036)
- Race conditions on certain platforms could cause the Instance Manager to try to restart the same instance multiple times. (Bug #18023)
- For a reference to a nonexistent index in `FORCE INDEX`, the error message referred to a column, not an index. (Bug #17873)
- The `sql_big_selects` system variable was not displayed by `SHOW VARIABLES`. (Bug #17849)
- `REPAIR TABLE` did not restore the length for packed keys in tables created under MySQL 4.x, which caused them to appear corrupt to `CHECK TABLE` but not to `REPAIR TABLE`. (Bug #17810)
- Results from `INFORMATION_SCHEMA.SCHEMATA` could contain uppercase information when `lower_case_table_names` was not 0. (Bug #17661)
- `CREATE TABLE ... SELECT` did not always produce the proper column default value in `TRADITIONAL` SQL mode. (Bug #17626)
- A range access optimizer heuristic was invalid, causing some queries to be much slower in MySQL 5.0 than in 4.0. (Bug #17379, Bug #18940)
- `mysqldump` would not dump views that had become invalid because a table named in the view definition had been dropped. Instead, it quit with an error message. Now you can specify the `--force` option to cause `mysqldump` to keep going and write an SQL comment containing the view definition to the dump output. (Bug #17371)
- The `--core-file-size` option for `mysqld_safe` was effective only for `root`. (Bug #17353)
- On Windows, multiple clients simultaneously attempting to perform `ALTER TABLE` operations on an `InnoDB` table could deadlock. (Bug #17264)
- Revised memory allocation for local objects within stored functions and triggers to avoid memory leak for repeated function or trigger invocation. (Bug #17260)
- Multiple calls to a stored procedure that selects from `INFORMATION_SCHEMA` could cause a server crash. (Bug #17204)

- Views created from prepared statements inside of stored procedures were created with a definition that included both `SQL_CACHE` and `SQL_NO_CACHE`. (Bug #17203)
- `mysqldump` wrote an extra pair of `DROP DATABASE` and `CREATE DATABASE` statements if run with the `--add-drop-database` option and the database contained views. (Bug #17201)
- A `Table ... doesn't exist` error could occur for statements that called a function defined in another database. (Bug #17199)
- For certain `CREATE TABLE ... SELECT` statements, the selected values were truncated when inserted into the new table. (Bug #17048)
- `ALTER TABLE` on a table created prior to 5.0.3 would cause table corruption if the `ALTER TABLE` did one of the following:
 - Change the default value of a column.
 - Change the table comment.
 - Change the table password.(Bug #17001)
- `MyISAM` table deadlock was possible if one thread issued a `LOCK TABLES` request for write locks and then an administrative statement such as `OPTIMIZE TABLE`, if between the two statements another client meanwhile issued a multiple-table `SELECT` for some of the locked tables. (Bug #16986)
- Symlinking `.mysql_history` to `/dev/null` to suppress statement history saving by `mysql` did not work. (`mysql` deleted the symlink and recreated `.mysql_history` as a regular file, and then wrote history to it.) (Bug #16803)
- Concatenating the results of multiple constant subselects produced incorrect results. (Bug #16716)
- Privilege checking on the contents of the `INFORMATION_SCHEMA.VIEWS` table was insufficiently restrictive. (Bug #16681)
- `mysqlcheck` tried to check views instead of ignoring them. (Bug #16502)
- `IS_USED_LOCK()` could return an incorrect connection identifier. (Bug #16501)
- Concurrent reading and writing of privilege structures could crash the server. (Bug #16372)
- Grant table modifications sometimes did not refresh the in-memory tables if the host name was `' '` or not specified. (Bug #16297)
- The `sql_notes` and `sql_warnings` system variables were not always displayed correctly by `SHOW VARIABLES` (for example, they were displayed as `ON` after being set to `OFF`). (Bug #16195)
- The `max_length` metadata value for columns created from `CONCAT()` could be incorrect when the collation of an argument differed from the collation of the `CONCAT()` itself. In some contexts such as `UNION`, this could lead to truncation of the column contents. (Bug #15962)
- The server no longer uses a signal handler for signal 0 because it could cause a crash on some platforms. (Bug #15869)
- `InnoDB` does not support `SPATIAL` indexes, but did not prevent creation of such an index. (Bug #15860)
- Long multiple-row `INSERT` statements could take a very long time for some multibyte character sets. (Bug #15811)

- The `system_time_zone` and `version_*` system variables could not be accessed using `SELECT @@var_name` syntax. (Bug #15684, Bug #12792)
- `EXPLAIN ... SELECT INTO` caused the client to hang. (Bug #15463)
- Nested natural joins worked executed correctly when executed as a nonprepared statement could fail with an `Unknown column 'col_name' in 'field list'` error when executed as a prepared statement, due to a name resolution problem. (Bug #15355)
- The `MD5()` and `SHA()` functions treat their arguments as case-sensitive strings. But when they are compared, their arguments were compared as case-insensitive strings, which leads to two function calls with different arguments (and thus different results) compared as being identical. This can lead to a wrong decision made in the range optimizer and thus to an incorrect result set. (Bug #15351)
- Invalid escape sequences in option files caused MySQL programs that read them to abort. (Bug #15328)
- Re-executing a stored procedure with a complex stored procedure cursor query could lead to a server crash. (Bug #15217)
- `CREATE TABLE ... SELECT ...` statements that used a stored function explicitly or implicitly (through a view) resulted in a `Table not locked` error. (Bug #15137, Bug #12472)
- An invalid comparison between keys with index prefixes over multibyte character fields could lead to incorrect result sets if the selected query execution plan used a range scan by an index prefix over a `UTF8` character field. This also caused incorrect results under similar circumstances with many other character sets. (Bug #14896)
- A view with a nonexistent account in the `DEFINER` clause caused `SHOW CREATE VIEW` to fail. Now `SHOW CREATE VIEW` issues a warning instead. (Bug #14875)
- For `BOOLEAN` mode full-text searches on nonindexed columns, `NULL` rows generated by a `LEFT JOIN` caused incorrect query results. (Bug #14708, Bug #25637)
- `SHOW CREATE TABLE` did not display the `AUTO_INCREMENT` column attribute if the SQL mode was `MYSQL323` or `MYSQL40`. This also affected `mysqldump`, which uses `SHOW CREATE TABLE` to get table definitions. (Bug #14515)
- Some queries were slower in 5.0 than in 4.1 because some 4.1 cost-evaluation code had not been merged into 5.0. (Bug #14292)
- The binary log lacked character set information for table names when dropping temporary tables. (Bug #14157)
- The result from `CONV()` is a string, but was not always treated the same way as a string when converted to a real value for an arithmetic operation. (Bug #13975)
- RPM packages had spurious dependencies on Perl modules and other programs. (Bug #13634)
- `REPLACE` statements caused activation of `UPDATE` triggers, not `DELETE` and `INSERT` triggers. (Bug #13479)
- With settings of `read_buffer_size` \geq 2G and `read_rnd_buffer_size` \geq 2G, `LOAD DATA INFILE` failed with no error message or caused a server crash for files larger than 2GB. (Bug #12982)
- A `B-TREE` index on a `MEMORY` table erroneously reported duplicate entry error for multiple `NULL` values. (Bug #12873)
- Use of `CONVERT_TZ()` in a stored function or trigger (or in a stored procedure called from a stored function or trigger) caused an error. (Bug #11081)

- `LOAD_FILE()` returned an error if the file did not exist, rather than `NULL` as it should according to the manual. (Bug #10418)
- When `myisamchk` needed to rebuild a table, `AUTO_INCREMENT` information was lost. (Bug #10405)
- For certain `CREATE VIEW` statements, the server did not detect invalid subqueries within the `SELECT` part. (Bug #7549)
- Within a trigger, `SET` statements used the SQL mode of the invoking statement, not the mode in effect at trigger creation time. (Bug #6951)
- Some queries that used `ORDER BY` and `LIMIT` performed quickly in MySQL 3.23, but slowly in MySQL 4.x/5.x due to an optimizer problem. (Bug #4981)
- The `basedir` and `tmpdir` system variables could not be accessed using `@@var_name` syntax. (Bug #1039)

Changes in MySQL 5.0.22 (2006-05-24)

This is a security fix release for the previous production release family.

This section documents all changes and bug fixes that have been applied since the last official MySQL release. If you would like to receive more fine-grained and personalized *update alerts* about fixes that are relevant to the version and features you use, please consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details, please see (<http://www.mysql.com/products/enterprise>).

Bugs Fixed

- **Security Fix:** An SQL-injection security hole has been found in multibyte encoding processing. The bug was in the server, incorrectly parsing the string escaped with the `mysql_real_escape_string()` C API function.

This vulnerability was discovered and reported by Josh Berkus <josh@postgresql.org> and Tom Lane <tgl@sss.pgh.pa.us> as part of the inter-project security collaboration of the OSDB consortium. For more information about SQL injection, please see the following text.

Discussion. An SQL injection security hole has been found in multibyte encoding processing. An SQL injection security hole can include a situation whereby when a user supplied data to be inserted into a database, the user might inject SQL statements into the data that the server will execute. With regards to this vulnerability, when character set-unaware escaping is used (for example, `addslashes()` in PHP), it is possible to bypass the escaping in some multibyte character sets (for example, SJIS, BIG5 and GBK). As a result, a function such as `addslashes()` is not able to prevent SQL-injection attacks. It is impossible to fix this on the server side. The best solution is for applications to use character set-aware escaping offered by a function such `mysql_real_escape_string()`.

However, a bug was detected in how the MySQL server parses the output of `mysql_real_escape_string()`. As a result, even when the character set-aware function `mysql_real_escape_string()` was used, SQL injection was possible. This bug has been fixed.

Workarounds. If you are unable to upgrade MySQL to a version that includes the fix for the bug in `mysql_real_escape_string()` parsing, but run MySQL 5.0.1 or higher, you can use the `NO_BACKSLASH_ESCAPES` SQL mode as a workaround. (This mode was introduced in MySQL 5.0.1.) `NO_BACKSLASH_ESCAPES` enables an SQL standard compatibility mode, where backslash is not considered a special character. The result will be that queries will fail.

To set this mode for the current connection, enter the following SQL statement:

```
SET sql_mode='NO_BACKSLASH_ESCAPES' ;
```

You can also set the mode globally for all clients:

```
SET GLOBAL sql_mode='NO_BACKSLASH_ESCAPES' ;
```

This SQL mode also can be enabled automatically when the server starts by using the command-line option `--sql-mode=NO_BACKSLASH_ESCAPES` or by setting `sql-mode=NO_BACKSLASH_ESCAPES` in the server option file (for example, `my.cnf` or `my.ini`, depending on your system). (Bug #8378, CVE-2006-2753)

References: See also: Bug #8303.

- **Replication:** The dropping of a temporary table whose name contained a backtick (``) character was not correctly written to the binary log, which also caused it not to be replicated correctly. (Bug #19188)
- The client libraries were not compiled for position-independent code on Solaris-SPARC and AMD x86_64 platforms. (Bug #18091, Bug #13159, Bug #14202)
- Running `myisampack` followed by `myisamchk` with the `--unpack` option would corrupt the `AUTO_INCREMENT` key. (Bug #12633)
- The patch for Bug #8303 broke the fix for Bug #8378 and was reverted.

In string literals with an escape character (\\) followed by a multibyte character that had (\\) as its second byte, the literal was not interpreted correctly. Now only next byte now is escaped, and not the entire multibyte character. This means it is a strict reverse of the `mysql_real_escape_string()` function.

Changes in MySQL 5.0.21 (2006-05-02)

This is a bugfix release for the current production release family.

This section documents all changes and bug fixes that have been applied since the last official MySQL release. If you would like to receive more fine-grained and personalized *update alerts* about fixes that are relevant to the version and features you use, please consider subscribing to *MySQL Enterprise* (a commercial MySQL offering). For more details, please see (<http://www.mysql.com/products/enterprise>).

This MySQL 5.0.21 release includes the patches for recently reported security vulnerabilities in the MySQL client/server protocol. We would like to thank Stefano Di Paola <stefano.dipaola@wisec.it> for finding and reporting these to us.

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- **Security Enhancement:** Added the global `max_prepared_stmt_count` system variable to limit the total number of prepared statements in the server. This limits the potential for denial-of-service attacks based on running the server out of memory by preparing huge numbers of statements. The current number of prepared statements is available through the `prepared_stmt_count` system variable. (Bug #16365)
- **MySQL Cluster:** It is now possible to perform a partial start of a cluster. That is, it is now possible to bring up the cluster without first running `ndbd --initial` on all configured data nodes. (Bug #18606)

- **MySQL Cluster:** Added the `--nowait-nodes` startup option for `ndbd`, making it possible to skip specified nodes without waiting for them to start when starting the cluster. See [ndbd — The MySQL Cluster Data Node Daemon](#).
- **MySQL Cluster:** It is now possible to install MySQL with Cluster support to a nondefault location and change the search path for font description files using either the `--basedir` or `--character-sets-dir` options. (Previously in MySQL 5.0, `ndbd` searched only the default path for character sets.)
- **Packaging:** The `MySQL-shared-compat-5.0.X-.i386.rpm` shared compatibility RPMs no longer contain libraries for MySQL 5.1. This avoids a conflict because the 5.0 and 5.1 libraries share the same soname number. They now contain libraries for MySQL 3.23, 4.0, 4.1, and 5.0 only. (Bug #19288)
- The default for the `innodb_thread_concurrency` system variable was changed to 8. (Bug #15868)
- Server and clients ignored the `--sysconfdir` option that was passed to `configure`. The directory specified by this option, if set, now is used as one of the standard locations in which to look for option files. (Bug #15069)
- In result set metadata, the `MYSQL_FIELD.length` value for `BIT` columns now is reported in number of bits. For example, the value for a `BIT(9)` column is 9. (Formerly, the value was related to number of bytes.) (Bug #13601)

Bugs Fixed

- **Security Fix:** Invalid arguments to `DATE_FORMAT()` caused a server crash. Thanks to Jean-David Maillefer for discovering and reporting this problem to the Debian project and to Christian Hammers from the Debian Team for notifying us of it. (Bug #20729, CVE-2006-3469)
- **Security Fix:** A malicious client, using specially crafted invalid `COM_TABLE_DUMP` packets was able to trigger an exploitable buffer overflow on the server. Thanks to Stefano Di Paola <stefano.dipaola@wisec.it> for finding and reporting this bug. (CVE-2006-1518)
- **Security Fix:** A malicious client, using specially crafted invalid login or `COM_TABLE_DUMP` packets was able to read uninitialized memory, which potentially, though unlikely in MySQL, could have led to an information disclosure. (,) Thanks to Stefano Di Paola <stefano.dipaola@wisec.it> for finding and reporting this bug. (CVE-2006-1516, CVE-2006-1517)
- **MySQL Cluster:** A simultaneous `DROP TABLE` and table update operation utilising a table scan could trigger a node failure. (Bug #18597)
- **MySQL Cluster:** When multiple node restarts were attempted without permitting each restart to complete, the error message returned was `Array index out of bounds` rather than `Too many crashed replicas`. (Bug #18349)
- **MySQL Cluster:** In a 2-node cluster with a node failure, restarting the node with a low value for `StartPartialTimeout` could cause the cluster to come up partitioned (“split-brain” issue).
A similar issue could occur when the cluster was first started with a sufficiently low value for this parameter. (Bug #16447, Bug #18612)
- **MySQL Cluster:** On systems with multiple network interfaces, data nodes would get “stuck” in startup phase 2 if the interface connecting them to the management server was working on node startup while the interface interconnecting the data nodes experienced a temporary outage. (Bug #15695)
- **MySQL Cluster:** On slow networks or CPUs, the management client `SHOW` command could sometimes erroneously show all data nodes as being master nodes belonging to nodegroup 0. (Bug #15530)
- **MySQL Cluster:** `TRUNCATE TABLE` did not reset the `AUTO_INCREMENT` counter for `MyISAM` tables when issued inside a stored procedure.

**Note**

This bug did not affect [InnoDB](#) tables.

In addition, `TRUNCATE TABLE` does not reset the `AUTO_INCREMENT` counter for [NDB](#) tables regardless of when it is called.

(Bug #14945)

References: See also: Bug #18864.

- **MySQL Cluster:** Unused open handlers for tables in which the metadata had changed were not properly closed. This could result in stale results from [NDB](#) tables following an `ALTER TABLE` statement. (Bug #13228)
- **MySQL Cluster:** Uninitialized internal variables could lead to unexpected results. (Bug #11033, Bug #11034)
- **MySQL Cluster:** When attempting to create an index on a [BIT](#) or [BLOB](#) column, `Error 743: Unsupported character set in table or index` was returned instead of `Error 906: Unsupported attribute type in index`.
- **Replication:** `CREATE VIEW` statements would not be replicated to the slave if the `--replicate-wild-ignore-table` rule was enabled. (Bug #18715)
- **Replication:** Updating a field value when also requesting a lock with `GET_LOCK()` would cause slave servers in a replication environment to terminate. (Bug #17284)
- [InnoDB](#) could read a delete mark from its system tables incorrectly. (Bug #19217)
- Corrected a syntax error in `mysql-test-run.sh`. (Bug #19190)
- Index corruption could occur in cases when `key_cache_block_size` was not a multiple of the `myisam-block-size` value (for example, with `--key_cache_block_size=1536` and `--myisam-block-size=1024`). (Bug #19079)
- The optimizer could cause a server crash or use a nonoptimal subset of indexes when evaluating whether to use `Index Merge/Intersection` variant of `index_merge` optimization. (Bug #19021)
- A missing `DEBUG_RETURN()` caused the server to emit a spurious error message: `missing DEBUG_RETURN or DEBUG_VOID_RETURN macro in function "open_table"`. (Bug #18964)
- Creating a table in an [InnoDB](#) database with a column name that matched the name of an internal [InnoDB](#) column (including `DB_ROW_ID`, `DB_TRX_ID`, `DB_ROLL_PTR` and `DB_MIX_ID`) would cause a crash. MySQL now returns `Error 1005 Cannot create table with errno set to -1`. (Bug #18934)
- MySQL would not compile on Linux distributions that use the `tinfo` library. (Bug #18912)
- `mysql_reconnect()` sent a `SET NAMES` statement to the server, even for pre-4.1 servers that do not understand the statement. (Bug #18830)
- For a reference to a nonexistent stored function in a stored routine that had a `CONTINUE` handler, the server continued as though a useful result had been returned, possibly resulting in a server crash. (Bug #18787)
- For single-`SELECT` union constructs of the form `(SELECT ... ORDER BY order_list1 [LIMIT n]) ORDER BY order_list2`, the `ORDER BY` lists were concatenated and the `LIMIT` clause was ignored. (Bug #18767)

- Conversion of a number to a `CHAR` `UNICODE` string returned an invalid result. (Bug #18691)
- `UNCOMPRESS(NULL)` could cause subsequent `UNCOMPRESS()` calls to return `NULL` for legal non-`NULL` arguments. (Bug #18643)
- If the second or third argument to `BETWEEN` was a constant expression such as `'2005-09-01 - INTERVAL 6 MONTH` and the other two arguments were columns, `BETWEEN` was evaluated incorrectly. (Bug #18618)
- A `LOCK TABLES` statement that failed could cause `MyISAM` not to update table statistics properly, causing a subsequent `CHECK TABLE` to report table corruption. (Bug #18544)
- The `yaSSL` library returned a cipher list in a manner incompatible with `OpenSSL`. (Bug #18399)
- `InnoDB` did not use a consistent read for `CREATE ... SELECT` when `innodb_locks_unsafe_for_binlog` was set. (Bug #18350)
- `DROP DATABASE` did not drop stored routines associated with the database if the database name was longer than 21 characters. (Bug #18344)
- The euro sign (€) was not stored correctly in columns using the `latin1_german1_ci` or `latin1_general_ci` collation. (Bug #18321)
- A recent change caused the `mysql` client not to display `NULL` values correctly and to display numeric columns left-justified rather than right-justified. The problems have been corrected. (Bug #18265)
- `COUNT(*)` on a `MyISAM` table could return different results for the base table and a view on the base table. (Bug #18237)
- `EXTRACT(QUARTER FROM date)` returned unexpected results. (Bug #18100)
- Executing `SELECT` on a large table that had been compressed within `myisampack` could cause a crash. (Bug #17917)
- Casting a string to `DECIMAL` worked, but casting a trimmed string (using `LTRIM()` or `RTRIM()`) resulted in loss of decimal digits. (Bug #17043)
- `mysql-test-run` could not be run as `root`. (Bug #17002)
- Queries of the form `SELECT DISTINCT timestamp_column WHERE date_function(timestamp_col) = constant` did not return all matching rows. (Bug #16710)
- IA-64 RPM packages for Red Hat and SuSE Linux that were built with the `icc` compiler incorrectly depended on `icc` runtime libraries. (Bug #16662)
- `MySQL-shared-compat-5.0.13-0.i386.rpm`, `MySQL-shared-compat-5.0.15-0.i386.rpm`, `MySQL-shared-compat-5.0.18-0.i386.rpm`, `MySQL-shared-compat-5.0.19-0.i386.rpm`, `MySQL-shared-compat-5.0.20-0.i386.rpm`, and `MySQL-shared-compat-5.0.20a-0.i386.rpm` incorrectly depended on `glibc 2.3` and could not be installed on a `glibc 2.2` system. (Bug #16539)
- The presence of multiple equalities in a condition after reading a constant table could cause the optimizer not to use an index. This resulted in certain queries being much slower than in MySQL 4.1. (Bug #16504)
- Within a trigger, `CONNECTION_ID()` did not return the connection ID of the thread that caused the trigger to be activated. (Bug #16461)

- For tables created in a MySQL 4.1 installation upgraded to MySQL 5.0 and up, multiple-table updates could update only the first matching row. (Bug #16281)
- A query using WHERE (*column_1*, *column_2*) IN ((*value_1*, *value_2*)[, (...), ...], (...), ...]) would return incorrect results. (Bug #16248)
- For `mysql.server`, if the `basedir` option was specified after `datadir` in an option file, the setting for `datadir` was ignored and assumed to be located under `basedir`. (Bug #16240)
- If the first argument to `BETWEEN` was a `DATE` or `TIME` column of a view and the other arguments were constants, `BETWEEN` did not perform conversion of the constants to the appropriate temporary type, resulting in incorrect evaluation. (Bug #16069)
- After calling `FLUSH STATUS`, the `max_used_connections` variable did not increment for existing connections and connections which use the thread cache. (Bug #15933)
- Lettercase in database name qualifiers was not consistently handled properly in queries when `lower_case_table_names` was set to 1. (Bug #15917)
- `DELETE` and `UPDATE` statements that used large `NOT IN (value_list)` clauses could use large amounts of memory. (Bug #15872)
- `InnoDB` failure to release an adaptive hash index latch could cause a server crash if the query cache was enabled. (Bug #15758)
- `LAST_INSERT_ID()` in a stored function or trigger returned zero. . (Bug #15728)
- `DELETE` with `LEFT JOIN` for `InnoDB` tables could crash the server if `innodb_locks_unsafe_for_binlog` was enabled. (Bug #15650)
- When running a query that contained a `GROUP_CONCAT(SELECT GROUP_CONCAT(...))`, the result was `NULL` except in the `ROLLUP` part of the result, if there was one. (Bug #15560)
- Use of `CONVERT_TZ()` in a view definition could result in spurious syntax or access errors. (Bug #15153)
- `CAST(double AS SIGNED INT)` for large `double` values outside the signed integer range truncated the result to be within range, but the result sometimes had the wrong sign, and no warning was generated. (Bug #15098)
- For `InnoDB` tables, an expression of the form `col_name BETWEEN col_name2 - INTERVAL x DAY AND col_name2 + INTERVAL x DAY` when used in a join returned incorrect results. (Bug #14360)
- Prevent recursive views caused by using `RENAME TABLE` on a view after creating it. (Bug #14308)
- `INSERT DELAYED` into a view caused an infinite loop. (Bug #13683)
- Avoid trying to include `<asm/atomic.h>` when it doesn't work in C++ code. (Bug #13621)
- Within stored routines, user names were parsed incorrectly if they were enclosed within quotation marks. (Bug #13310)
- The server was always built as though `--with-extra-charsets=complex` had been specified. (Bug #12076)

Changes in MySQL 5.0.20a (2006-04-18)

This is a bugfix release for the current production release family. It replaces MySQL 5.0.20.

- [Additional SSL Support Information](#)
- [Bugs Fixed](#)

Additional SSL Support Information

- Please note that the original 5.0.20 announcement included inexact wording: SSL support is “included” in both server and client, but by default not “enabled”. SSL can be enabled by passing the SSL-related options (`--ssl`, `--ssl-key=...`, `--ssl-cert=...`, `--ssl-ca=...`) when starting the server and the client or by specifying these options in an option file. For more information, see [Using Secure Connections](#).
- With version 5.0.20a, SSL support is contained in all binaries for all Unix (including Linux) and Windows platforms except AIX, HP-UX, OpenServer 6, and the RPMs specific for RHAS3/RHAS4/SLES9 on Itanium CPUs ([ia64](#)). It is also not contained in those for Novell Netware.

Bugs Fixed

- The fix for “Command line options are ignored for mysql client” has been revoked because it introduced an incompatible change in the way the `mysql` command-line client selects the server to connect to. In the worst case, this might have led to a client issuing commands to a server for which they were not intended, and this must not happen. To help all users in understanding this subject, [Invoking MySQL Programs](#) now includes additional explanation of how command options function with regard to host selection. (Bug #16855)
- The code of the yaSSL library has been improved to avoid a dependency on a C++ runtime library, so a link with pure C applications is now possible on additional (but not yet all) platforms. We are working on fixing the remaining issues.

Changes in MySQL 5.0.20 (2006-03-31)

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- **MySQL Cluster:** The `NDBCLUSTER` storage engine now supports `INSERT IGNORE` and `REPLACE` statements. Previously, these statements failed with an error. (Bug #17431)
- **Replication:** Triggers from older servers that included no `DEFINER` clause in the trigger definition now execute with the privileges of the invoker (which on the slave is the slave SQL thread). Previously, replication slaves could not replicate such triggers. (Bug #16266)
- Builds for Windows, Linux, and Unix (except AIX) platforms now have SSL support enabled, in the server as well as in the client libraries. Because part of the SSL code is written in C++, this does introduce dependencies on the system's C++ runtime libraries in several cases, depending on compiler specifics. (Bug #18195)
- Large file support added to build for `QNX` platform. (Bug #17336)
- **InnoDB:** The `InnoDB` storage engine now provides a descriptive error message if `ibdata` file information is omitted from `my.cnf`. (Bug #16827)
- Added the `--sysdate-is-now` option to `mysqld` to enable `SYSDATE()` to be treated as an alias for `NOW()`. See [Date and Time Functions](#). (Bug #15101)
- Large file support was re-enabled for the MySQL server binary for the AIX 5.2 platform. (Bug #13571)

- The syntax for `CREATE PROCEDURE` and `CREATE FUNCTION` statements now includes a `DEFINER` clause. The `DEFINER` value specifies the security context to be used when checking access privileges at routine invocation time if the routine has the `SQL SECURITY DEFINER` characteristic. See [CREATE PROCEDURE and CREATE FUNCTION Syntax](#), for more information.

When `mysqldump` is invoked with the `--routines` option, it now dumps the `DEFINER` value for stored routines.

Bugs Fixed

- **MySQL Cluster:** A timeout in the handling of an `ABORT` condition with more than 32 operations could yield a node failure. (Bug #18414)
- **MySQL Cluster:** A node restart immediately following a `CREATE TABLE` failed.



Important

This fix supports 2-node Clusters only.

(Bug #18385)

- **MySQL Cluster:** In event of a node failure during a rollback, a “false” lock could be established on the backup for that node, which lock could not be removed without restarting the node. (Bug #18352)
- **MySQL Cluster:** The cluster created a crashed replica of a table having an ordered index—or when logging was not enabled, of a table having a table or unique index—leading to a crash of the cluster following 8 successive restarts. (Bug #18298)
- **MySQL Cluster:** When replacing a failed master node, the replacement node could cause the cluster to crash from a buffer overflow if it had an excessively large amount of data to write to the cluster log. (Bug #18118)
- **MySQL Cluster:** Certain queries using `ORDER BY ... ASC` in the `WHERE` clause could return incorrect results. (Bug #17729)
- **MySQL Cluster:** If a `mysql` or other client could not parse the result set returned from a `mysqld` process acting as an SQL node in a cluster, the client would crash instead of returning the appropriate error. For example, this could happen when the client attempted to use a character set was not available to the `mysqld`. (Bug #17380)
- **MySQL Cluster:** Some query cache statistics were not always correctly reported for Cluster tables. (Bug #16795)
- **MySQL Cluster:** Restarting nodes were permitted to start and join the cluster too early. (Bug #16772)
- **MySQL Cluster:** Inserting and deleting `BLOB` column values while a backup was in process could cause data nodes to shut down. (Bug #14028)
- **MySQL Cluster:** The server would not compile with `NDB` support on AIX 5.2. (Bug #10776)
- **Replication:** Use of `TRUNCATE TABLE` for a `TEMPORARY` table on a master server was propagated to slaves properly, but slaves did not decrement the `Slave_open_temp_tables` counter properly. (Bug #17137)
- **Replication:** The `DEFINER` value for stored routines was not replicated. (Bug #15963)
- A `SELECT ... ORDER BY ...` from a view defined using a function could crash the server. An example of such a view is `CREATE VIEW v1 AS SELECT SQRT(c1) FROM t1`. (Bug #18386)

- [InnoDB](#) had a memory leak for duplicate-key errors with tables having 90 columns or more. (Bug #18384)
- A `DELETE` using a subquery could crash the server. (Bug #18306)
- If a row was inserted inside a stored procedure using the parameters passed to the procedure in the `INSERT` statement, the resulting binary log entry was not escaped properly. (Bug #18293)
- If [InnoDB](#) encountered a `ER_LOCK_TABLE_FULL` error and rolled back a transaction, the transaction was still written to the binary log. (Bug #18283)
- When using `ORDER BY` with a nonstring column inside `GROUP_CONCAT()` the result's character set was converted to binary. (Bug #18281)

References: See also: Bug #14169.

- Complex queries with nested joins could cause a server crash. (Bug #18279)
- For [InnoDB](#) tables created in MySQL 4.1 or earlier, or created in 5.0 or later with compact format, updating a row so that a long column is updated or the length of some column changes, [InnoDB](#) later failed to reclaim the `BLOB` storage space if the row was deleted. (Bug #18252)
- If [InnoDB](#) ran out of buffer space for row locks and adaptive hashes, the server would crash. Now [InnoDB](#) rolls back the transaction. (Bug #18238)
- Views that incorporated tables from the `INFORMATION_SCHEMA` database resulted in a server crash when queried. (Bug #18224)
- `REPAIR TABLE`, `OPTIMIZE TABLE`, and `ALTER TABLE` operations on transactional tables (or on tables of any type on Windows) could corrupt triggers associated with those tables. (Bug #18153)
- The server could deadlock under heavy load while writing to the binary log. (Bug #18116)
- A `SELECT *` query on an `INFORMATION_SCHEMA` table by a user with limited privileges resulted in a server crash. (Bug #18113)
- Connecting to a server with a UCS2 default character set with a client using a non-UCS2 character set crashed the server. (Bug #18004)
- [MyISAM](#): Performing a bulk insert on a table referenced by a trigger would crash the table. (Bug #17764)
- Updating a view that filters certain rows to set a filtered out row to be included in the table caused infinite loop. For example, if the view has a `WHERE` clause of `salary > 100` then issuing an `UPDATE` statement of `SET salary = 200 WHERE id = 10`, caused an infinite loop. (Bug #17726)
- [MyISAM](#): Keys for which the first part of the key was a `CHAR` or `VARCHAR` column using the UTF-8 character set and longer than 254 bytes could become corrupted. (Bug #17705)
- Updating the value of a Unicode `VARCHAR` column with the result returned by a stored function would cause the insertion of ASCII characters into the column instead of Unicode, even where the function's return type was also declared as Unicode. (Bug #17615)
- For `FEDERATED` tables, a `SELECT` statement with an `ORDER BY` clause did not return rows in the proper order. (Bug #17377)
- `SELECT ... WHERE column LIKE 'A%'`, when `column` had a key and used the `latin2_czech_cs` collation, caused the wrong number of rows to be returned. (Bug #17374)
- A `LEFT JOIN` with a `UNION` that selects literal values could crash the server. (Bug #17366)

- Checks for permissions on database operations could be performed in a case-insensitive manner (a user with permissions on database `MYDATABASE` could by accident get permissions on database `myDataBase`), if the privilege data were still cached from a previous check. (Bug #17279)
- Stored procedures that call UDFs and pass local string variables caused server crashes. (Bug #17261)
- If the `WHERE` condition of a query contained an `OR`-ed `FALSE` term, the set of tables whose rows cannot serve for null-complements in outer joins was determined incorrectly. This resulted in blocking possible conversions of outer joins into joins by the optimizer for such queries. (Bug #17164)
- `InnoDB` tables with an adaptive hash blocked other queries during `CHECK TABLE` statements while the entire hash was checked. This could be a long time for a large hash. (Bug #17126)
- Stored routine names longer than 64 characters were silently truncated. Now the limit is properly enforced and an error occurs. (Bug #17015)
- `InnoDB`: The `LATEST FOREIGN KEY ERROR` section in the output of `SHOW INNODB STATUS` was sometimes formatted incorrectly, causing problems with scripts that parsed the output of this statement. (Bug #16814)
- If the server was started with the `--skip-grant-tables` option, it was impossible to create a trigger or a view without explicitly specifying a `DEFINER` clause. (Bug #16777)
- The `FORMAT()` function returned an incorrect result when the client's `character_set_connection` value was `utf8`. (Bug #16678)
- Using `ORDER BY intvar` within a stored procedure (where `intvar` is an integer variable or expression) would crash the server.



Note

The use of an integer `i` in an `ORDER BY i` clause for sorting the result by the `i`th column is deprecated (and nonstandard). It should *not* be used in new applications. See [SELECT Syntax](#).

(Bug #16474)

- Character set conversion of string constants for `UNION` of constant and table column was not done when it was safe to do so. (Bug #15949)
- Triggers created in MySQL 5.0.16 and earlier could not be dropped after upgrading the server to 5.0.17 or later. (Bug #15921)
- The `mysql_close()` C API function leaked handles for shared-memory connections on Windows. (Bug #15846)
- `COUNT(DISTINCT col1, col2)` and `COUNT(DISTINCT CONCAT(col1, col2))` operations produced different results if one of the columns was an indexed `DECIMAL` column. (Bug #15745)
- A `SELECT` using a function against a nested view would crash the server. (Bug #15683)
- The server displayed garbage in the error message warning about bad assignments to `DECIMAL` columns or routine variables. (Bug #15480)
- During conversion from one character set to `ucs2`, multibyte characters with no `ucs2` equivalent were converted to multiple characters, rather than to `0x003F QUESTION MARK`. (Bug #15375)
- Certain combinations of joins with mixed `ON` and `USING` clauseds caused `unknown column` errors. (Bug #15229)

- `SELECT COUNT(*)` for a `MyISAM` table could return different results depending on whether an index was used. (Bug #14980)
- Attempting to access an `InnoDB` table after starting the server with `--skip-innodb` caused a server crash. (Bug #14575)
- Use of stored functions with `DISTINCT` or `GROUP BY` can produce incorrect results when `ORDER BY` is also used. (Bug #13575)
- The server would execute stored routines that had a nonexistent definer. (Bug #13198)
- `mysql_config` returned incorrect libraries on `x86_64` systems. (Bug #13158)
- Loading of UDFs in a statically linked MySQL caused a server crash. UDF loading is now blocked if the MySQL server is statically linked. (Bug #11835)

Changes in MySQL 5.0.19 (2006-03-04)

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- **Incompatible Change:** The `InnoDB` storage engine no longer ignores trailing spaces when comparing `BINARY` or `VARBINARY` column values. This means that (for example) the binary values `'a'` and `'a '` are now regarded as *unequal* any time they are compared, as they are in `MyISAM` tables.

See [The BINARY and VARBINARY Types](#) for more information about the `BINARY` and `VARBINARY` types. (Bug #14189)
- **MySQL Cluster:** More descriptive warnings are now issued when inappropriate logging parameters are set in `config.ini`. (Formerly, the warning issued was simply `Could not add logfile destination.`) (Bug #11331)
- **MySQL Cluster:** The `ndb_mgm` client commands `node_id START` and `node_id STOP` now work with management nodes as well as data nodes. However, using `ALL` for `node_id` continues to affect all data nodes only.
- `mysql` no longer terminates data value display when it encounters a NUL byte. Instead, it displays NUL bytes as spaces. (Bug #16859)
- New `charset` command added to `mysql` command-line client. By typing `charset name` or `\C name` (such as `\C UTF8`), the client character set can be changed without reconnecting. (Bug #16217)
- Added the `--wait-timeout` option to `mysqlmanager` to enable configuration of the timeout for dropping an inactive connection, and increased the default timeout from 30 seconds to 28,800 seconds (8 hours). (Bug #15980, Bug #12674)
- The `INFORMATION_SCHEMA` now skips data contained in unlistable/unreadable directories rather than returning an error. (Bug #15851)
- `InnoDB` now caches a list of unflushed files instead of scanning for unflushed files during a table flush operation. This improves performance when `--innodb_file_per_table` is set on a system with a large number of `InnoDB` tables. (Bug #15653)
- Added the `--port-open-timeout` option to `mysqld` to control how many seconds the server should wait for the TCP/IP port to become free if it cannot be opened. (Bug #15591)

- Wording of error 1329 changed to `No data - zero rows fetched, selected, or processed.` (Bug #15206)
- The message for error 1109 changed from `Unknown table ... in order clause` to `Unknown table ... in field list.` (Bug #15091)
- A number of performance issues were resolved that had previously been encountered when using statements that repeatedly invoked stored functions. For example, calling `BENCHMARK()` using a stored function executed much more slowly than when invoking it with inline code that accomplished the same task. In most cases the two should now execute with approximately the same speed. (Bug #14946, Bug #15014)
- `mysqldump` now surrounds the `DEFINER`, `SQL SECURITY DEFINER` and `WITH CHECK OPTION` clauses of a `CREATE VIEW` statement with "not in version" comments to prevent errors in earlier versions of MySQL. (Bug #14871)
- When using the `GROUP_CONCAT()` function where the `group_concat_max_len` system variable was greater than 512, the result type differed depending on whether an `ORDER BY` clause was included: `BLOB` if it was, `VARBINARY` if it was not. (For nonbinary string arguments, the result was `TEXT` or `VARCHAR`.)

Now an `ORDER BY` does not affect the result, which is `VARBINARY (VARCHAR)` only if `group_concat_max_len` is less than or equal to 512, `BLOB (TEXT)` otherwise. (Bug #14169)
- The `mysql_ping()` function will now retry if the `reconnect` flag is set and error `CR_SERVER_LOST` is encountered during the first attempt to ping the server. (Bug #14057)
- The `mysqltest` utility now converts all `CR/LF` combinations to `LF` to enable test cases intended for Windows to work properly on UNIX-like systems. (Bug #13809)
- `libmysqlclient` now uses versioned symbols with GNU ld. (Bug #3074)
- The client API now attempts to reconnect using TCP/IP if the `reconnect` flag is set, as is the case with sockets. (Bug #2845)
- Two new Hungarian collations are included: `utf8_hungarian_ci` and `ucs2_hungarian_ci`. These support the correct sort order for Hungarian vowels. However, they do not support the correct order for sorting Hungarian consonant contractions; we expect to fix this issue in a future release.
- Several changes were made to make upgrades easier:
 - Added the `mysql_upgrade` program that checks all tables for incompatibilities with the current version of MySQL Server and repairs them if necessary. This program should be run for each MySQL upgrade (rather than `mysql_fix_privilege_tables`). See [mysql_upgrade — Check Tables for MySQL Upgrade](#).
 - Added the `FOR UPGRADE` option for the `CHECK TABLE` statement. This option checks whether tables are incompatible with the current version of MySQL Server.
 - Added the `--check-upgrade` to `mysqlcheck` that invokes `CHECK TABLE` with the `FOR UPGRADE` option.

Bugs Fixed

- **MySQL Cluster:** Cluster log file paths were truncated to 128 characters. They may now be as long as `MAX_PATH` (the maximum path length permitted by the operating system). (Bug #17411)
- **MySQL Cluster:** Following multiple forced shutdowns and restarts of data nodes, `DROP DATABASE` could fail. (Bug #17325)

- **MySQL Cluster:** The `REDO` log would become corrupted (and thus unreadable) in some circumstances, due to a failure in the query handler. (Bug #17295)
- **MySQL Cluster:** An `UPDATE` with an inner join failed to match any records if both tables in the join did not have a primary key. (Bug #17257)
- **MySQL Cluster:** A `DELETE` with a join in the `WHERE` clause failed to retrieve any records if both tables in the join did not have a primary key. (Bug #17249)
- **MySQL Cluster:** The error message returned by `perror --ndb` was prefixed with `OS error code` instead of `NDB error code`. (Bug #17235)
- **MySQL Cluster:** In some cases, `LOAD DATA INFILE` did not load all data into `NDB` tables. (Bug #17081)
- **MySQL Cluster:** `ndb_delete_all` ran out of memory when processing tables containing `BLOB` columns. (Bug #16693)
- **MySQL Cluster:** A `BIT` column whose offset and length totaled 32 caused the cluster to crash. (Bug #16125)
- **MySQL Cluster:** `UNIQUE` keys in Cluster tables were limited to 225 bytes in length. (Bug #15918)
- **MySQL Cluster:** The `ndb_autodiscover` test failed sporadically due to a node not being permitted to connect to the cluster. (Bug #15619)
- **MySQL Cluster:** `NDB` returned an incorrect `Can't find file error` for OS error 24; this has been changed to `Too many open files`. (Bug #15020)
- **MySQL Cluster:** No error message was generated for setting `NoOfFragmentLogFiles` too low. (Bug #13966)
- **MySQL Cluster:** No error message was generated for setting `MaxNoOfAttributes` too low. (Bug #13965)
- **MySQL Cluster:** When running more than one management process in a cluster:
 - `ndb_mgm -c host:port -e "node_id STOP"` stopped a management process running only on the same system where the command was issued.
 - `ndb_mgm -e "SHUTDOWN"` failed to shut down any management processes at all.
(Bug #12045, Bug #12124)
- **MySQL Cluster:** `ndb_mgm -c host:port -e "node_id STOP"` would stop a management process running only on the same system on which the command was issued.
- **MySQL Cluster:** `ndb_mgm -e "SHUTDOWN"` failed to shut down any management processes at all.
- **Replication:** For a transaction that used `MyISAM` and `InnoDB` tables, interruption of the transaction due to a dropped connection on a master server caused slaves to lose synchrony. (Bug #16559)
- **Replication:** The `--replicate-do` and `--replicate-ignore` options were not being enforced on multiple-table statements. (Bug #16487, Bug #15699)
- **Replication:** Previously, a stored function invocation was written to the binary log as `DO func_name()` if the invocation changes data and occurs within a nonlogged statement, or if the function invokes a stored procedure that produces an error. These invocations now are logged as `SELECT func_name()`

instead for better control over error code checking (slave servers could stop due to detecting a different error than occurred on the master). (Bug #14769)

- **Replication:** `BIT` fields were not properly handled when using row-based replication. (Bug #13418)
- **Cluster API:** Upon the completion of a scan where a key request remained outstanding on the primary replica and a starting node died, the scan did not terminate. This caused incomplete error handling for the failed node. (Bug #15908)
- `type_decimal` failed with the prepared statement protocol. (Bug #17826)
- The MySQL server could crash with out of memory errors when performing aggregate functions on a `DECIMAL` column. (Bug #17602)
- Using `DROP FUNCTION IF EXISTS func_name` to drop a user-defined function caused a server crash if the server was running with the `--skip-grant-tables` option. (Bug #17595)
- Data truncations on non-`UNIQUE` indexes could crash `InnoDB` when using multibyte character sets. (Bug #17530)
- A natural join between `INFORMATION_SCHEMA` tables failed. (Bug #17523)
- A stored procedure failed to return data the first time it was called per connection. (Bug #17476)
- For certain `MERGE` tables, the optimizer wrongly assumed that using `index_merge/intersection` was too expensive. (Bug #17314)
- The parser permitted `CREATE AGGREGATE FUNCTION` for creating stored functions, even though `AGGREGATE` does not apply. (It is used only for `CREATE FUNCTION` only when creating user-defined functions.) (Bug #16896)
- Cursors in stored routines could cause a server crash. (Bug #16887)
- Triggers created without `BEGIN` and `END` clauses resulted in “You have an error in your SQL syntax” errors when dumping and replaying a binary log. (Bug #16878)
- Using `ALTER TABLE` to increase the length of a `BINARY(M)` column caused column values to be padded with spaces rather than `0x00` bytes. (Bug #16857)
- A `RETURN` statement within a trigger caused a server crash. `RETURN` is no longer permitted within triggers. To exit immediately, use `LEAVE`. (Bug #16829)
- For a MySQL 5.0 server, using MySQL 4.1 tables in queries with a `GROUP BY` clause could result in buffer overrun or a server crash. (Bug #16752)
- An `INSERT` statement in a stored procedure corrupted the binary log. (Bug #16621)
- If the query optimizer transformed a `GROUP BY` clause in a subquery, it did not also transform the `HAVING` clause if there was one, producing incorrect results. (Bug #16603)
- In a highly concurrent environment, a server crash or deadlock could result from execution of a statement that used stored functions or activated triggers coincident with alteration of the tables used by these functions or triggers. (Bug #16593)
- A race condition could occur when dropping the adaptive hash index for a B-tree page in `InnoDB`. (Bug #16582)
- When evaluation of the test in a `CASE` failed in a stored procedure that contained a `CONTINUE` handler, execution resumed at the beginning of the `CASE` statement instead of at the end. (Bug #16568)

- Clients compiled from source with the `--without-readline` did not save command history from session to session. (Bug #16557)
- The `DECIMAL` data type was not being handled correctly with prepared statements. (Bug #16511)
- Instance Manager searched wrong location for password file on some platforms. (Bug #16499)
- `UPDATE` statement crashed multibyte character set `FULLTEXT` index if update value was almost identical to initial value only differing in some spaces being changed to ` `. (Bug #16489)
- Certain nested `LEFT JOIN` operations were not properly optimized. (Bug #16393)
- Dropping `InnoDB` constraints named `tbl_name_ibfk_0` could crash the server. (Bug #16387)
- `SELECT` with `GROUP BY` on a view could cause a server crash. (Bug #16382)
- An invalid stored routine could not be dropped. (Bug #16303)
- `InnoDB`: After upgrading an `InnoDB` table having a `VARCHAR BINARY` column created in MySQL 4.0 to MySQL 5.0, update operations on the table would cause the server to crash. (Bug #16298)
- Parallel builds occasionally failed on Solaris. (Bug #16282)
- A call to the `IF()` function using decimal arguments could return incorrect results. (Bug #16272)
- MySQL server dropped client connection for certain `SELECT` statements against views defined that used `MERGE` algorithm. (Bug #16260)
- `InnoDB` used full explicit table locks in trigger processing. (Bug #16229)
- Using `GROUP BY` on column used in `WHERE` clause could cause empty set to be returned. (Bug #16203)
- A memory leak caused warnings on slaves for certain statements that executed without warning on the master. (Bug #16175)
- The `FORCE INDEX` keyword in a query would prevent an index merge from being used where an index merge would normally be chosen by the optimizer. (Bug #16166)
- Setting `InnoDB` path settings to an empty string caused `InnoDB` storage engine to crash upon server startup. (Bug #16157)
- The `mysql_stmt_sqlstate()` C API function incorrectly returned an empty string rather than `'00000'` when no error occurred. (Bug #16143)
- `MIN()` and `MAX()` operations were not optimized for views. (Bug #16016)
- Performing a `RENAME TABLE` on an `InnoDB` table when the server was started with the `--innodb_file_per_table` option and the data directory was a symlink caused a server crash. (Bug #15991)
- Executing a `SHOW CREATE VIEW` query of an invalid view caused the `mysql_next_result()` function of `libMySQL.dll` to hang. (Bug #15943)
- Test suite `sp` test left behind tables when the test failed that could cause future tests to fail. (Bug #15866)
- `STR_TO_DATE(1, NULL)` caused a server crash. (Bug #15828, CVE-2006-3081)
- `CAST(... AS TIME)` operations returned different results when using versus not using prepared-statement protocol. (Bug #15805)

- Issuing a `DROP USER` statement could cause some users to encounter a `hostname is not permitted to connect to this MySQL server` error. (Bug #15775)
- The contents of `fill_help_tables.sql` could not be loaded in strict SQL mode. (Bug #15760)
- `fill_help_tables.sql` was not included in binary distributions for several platforms. (Bug #15759)
- Certain `LEAVE` statements in stored procedures were not properly optimized. (Bug #15737)
- The `mysql_real_connect()` C API function incorrectly reset the `MYSQL_OPT_RECONNECT` option to its default value. (Bug #15719)
- Created a user function with an empty string (that is, `CREATE FUNCTION ''()`), was accepted by the server. Following this, calling `SHOW FUNCTION STATUS` would cause the server to crash. (Bug #15658)
- Trying to compile the server on Windows generated a stack overflow warning due to a recursive definition of the internal `Field_date::store()` method. (Bug #15634)
- In some cases the query optimizer did not properly perform multiple joins where inner joins followed left joins, resulting in corrupted result sets. (Bug #15633)
- Certain permission management statements could create a `NULL` host name for a user, resulting in a server crash. (Bug #15598)
- Improper memory handling for stored routine variables could cause memory overruns and binary log corruption. (Bug #15588)
- The `COALESCE()` function truncated data in a `TINYTEXT` column. (Bug #15581)
- Binary distributions for Solaris contained files with group ownership set to the nonexisting `wheel` group. Now the `bin` group is used. (Bug #15562)
- The absence of a table in the left part of a left or right join was not checked prior to name resolution, which resulted in a server crash. (Bug #15538)
- A `SELECT` of a stored function that references the `INFORMATION_SCHEMA` could crash the server. (Bug #15533)
- Characters in the `gb2312` and `euckr` character sets which did not have Unicode mappings were truncated. (Bug #15377)
- Certain subqueries where the inner query was the result of an aggregate function would return different results with MySQL 5.0 or 5.1 than with MySQL 4.1.
Subselects could also return wrong results when the query cache and grouping were involved. (Bug #15347)
- Performing an `ORDER BY` on an indexed `ENUM` column returned error. (Bug #15308)
- A `SELECT` query which contained a `GROUP_CONCAT()` and an `ORDER BY` clause against the `INFORMATION_SCHEMA` resulted in an empty result set. (Bug #15307)
- The `NOT FOUND` condition handler for stored procedures did not distinguish between a `NOT FOUND` condition and an exception or warning. (Bug #15231)
- The `SELECT` privilege was required for triggers that performed no selects. (Bug #15196)
- An attempt to open a table that requires a disabled storage engine could cause a server crash. (Bug #15185)

- The `UPDATE` privilege was required for triggers that performed no updates. (Bug #15166)
- Tarball install package was missing a proper `fill_help_tables.sql` file. (Bug #15151)
- Setting `innodb_log_file_size` to a value greater than 4G crashed the server. (Bug #15108)
- When multiple handlers are created for the same MySQL error number within nested blocks, the outermost handler took precedence. (Bug #15011)
- A statement containing `GROUP BY` and `HAVING` clauses could return incorrect results when the `HAVING` clause contained logic that returned `FALSE` for every row. (Bug #14927)
- Stored routines that contained only a single statement were not written properly to the dumpfile when using `mysqldump`. (Bug #14857)
- Killing a long-running query containing a subquery could cause a server crash. (Bug #14851)
- `GRANT` statements specifying schema names that included underscore characters (that is, `my_schema`) did not match if the underscore was escaped in the `GRANT` statement (that is, `GRANT ALL ON `my_schema` . . .`). (Bug #14834)
- Generating an `AUTO_INCREMENT` value through a `FEDERATED` table did not set the value returned by `LAST_INSERT_ID()`. (Bug #14768)
- `SUBSTRING_INDEX()` could yield inconsistent results when applied with the same arguments to consecutive rows in a query. (Bug #14676)
- Running out of disk space in the location specified by the `tmpdir` option resulted in incorrect error message. (Bug #14634)
- `InnoDB`: Comparison of indexed `VARCHAR CHARACTER SET ucs2 COLLATE ucs2_bin` columns using `LIKE` could fail. (Bug #14583)
- A stored procedure with an undefined variable and an exception handler would hang the client when called. (Bug #14498)
- A `FULLTEXT` query in a prepared statement could result in unexpected behavior. (Bug #14496)
- Using an aggregate function as the argument for a `HAVING` clause resulted in the aggregate function always returning `FALSE`. (Bug #14274)
- The use of `LOAD INDEX` within a stored routine was permitted and caused the server to crash.

**Note**

`LOAD INDEX` statements within stored routines *are not supported*, and now yield an error if attempted. This behavior is intended.

(Bug #14270)

- A `COMMIT` statement followed by a `ALTER TABLE` statement on a BDB table caused server crash. (Bug #14212)
- The `mysql_stmt_store_result()` C API function could not be used for a prepared statement if a cursor had been opened for the statement. (Bug #14013)
- `SET sql_mode = N`, where $N > 31$, did not work properly. (Bug #13897)
- Attempts to create `FULLTEXT` indexes on `VARCHAR` columns larger than 1000 bytes resulted in error. (Bug #13835)

- The `RENAME TABLE` statement did not move triggers to the new table. (Bug #13525)
- The length of a `VARCHAR()` column that used the `utf8` character set would increase each time the table was re-created in a stored procedure or prepared statement, eventually causing the `CREATE TABLE` statement to fail. (Bug #13134)
- Instance Manager erroneously accepted a list of instance identifiers for the `START INSTANCE` and `STOP INSTANCE` commands (should accept only a single identifier). (Bug #12813)
- A prepared statement created from a `SELECT ... LIKE` query (such as `PREPARE stmt1 FROM 'SELECT col_1 FROM tedd_test WHERE col_1 LIKE ?';`) would begin to produce erratic results after being executed repeatedly numerous (thousands) of times. (Bug #12734)
- Multibyte path names for `LOAD DATA` and `SELECT ... INTO OUTFILE` caused errors. Added the `character_set_filesystem` system variable, which controls the interpretation of string literals that refer to file names. (Bug #12448)
- Temporary table aliasing did not work inside stored functions. (Bug #12198)
- The embedded server did not permit binding of columns to the `MYSQL_TYPE_VAR_STRING` data type in prepared statements. (Bug #12070)
- When Connector/ODBC or any other client called `my_init()/my_end()` several times, it caused corruption of charset data stored in `once_mem_pool`. (Bug #11892)
- Setting the `myisam_repair_threads` system variable to a value larger than 1 could cause corruption of large `MyISAM` tables. (Bug #11527)
- The `mysqlbinlog` utility did not output `DELIMITER` statements, causing syntax errors for stored routine creation statements. (Bug #11312)
- The embedded server failed various tests in the automated test suite. (Bug #10801, Bug #10925, Bug #15433, Bug #9633, Bug #10926, Bug #9631, Bug #10930, Bug #10911, Bug #9630, Bug #10924)
- A large `BIGINT` value specified in a `WHERE` clause could be treated differently depending on whether it is specified as a quoted string. (For example, `WHERE bigint_col = 1766600000000000000` versus `WHERE bigint_col = '1766600000000000000'`). (Bug #9088)
- `CHECKSUM TABLE` returned different values for `MyISAM` tables depending on whether the `QUICK` or `EXTENDED` option was used. (Bug #8841)
- Using the `TRUNCATE()` function with a negative number for the second argument on a `BIGINT` column returned incorrect results. (Bug #8461)
- Issuing `GRANT EXECUTE` on a procedure would display any warnings related to the creation of the procedure. (Bug #7787)
- Repeated invocation of `my_init()` and `my_end()` caused corruption of character set data and connection failure. (Bug #6536)
- An `INSERT ... SELECT` statement between tables in a `MERGE` set can return errors when statement involves insert into child table from merge table or vice-versa. (Bug #5390)

Changes in MySQL 5.0.18 (2005-12-21)

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- The server treats stored routine parameters and local variables (and stored function return values) according to standard SQL. Previously, parameters, variables, and return values were treated as items in expressions and were subject to automatic (silent) conversion and truncation. Now the data type is observed. Data type conversion and overflow problems that occur in assignments result in warnings, or errors in strict mode. The `CHARACTER SET` clause for character data type declarations is used. Parameters, variables, and return values must be scalars; it is no longer possible to assign a row value. Also, stored functions execute using the `sql_mode` value in force at function creation time rather than ignoring it. For more information, see [CREATE PROCEDURE and CREATE FUNCTION Syntax](#). (Bug #13808, Bug #12903, Bug #9078, Bug #14161, Bug #13705, Bug #13909, Bug #15148, Bug #8769, Bug #8702, Bug #9572, Bug #8768)
- It is now possible to build the server such that `MyISAM` tables can support up to 128 keys rather than the standard 64. This can be done by configuring the build using the option `--with-max-indexes=N`, where $N \leq 128$ is the maximum number of indexes to permit per table. (Bug #10932)

Bugs Fixed

- **MySQL Cluster:** If an abort by the Transaction Coordinator timed out, the abort condition was incorrectly handled, causing the transaction record to be released prematurely. (Bug #15685)
- **MySQL Cluster:** The `ndb_read_multi_range.test` script failed to drop a table, causing the test to fail. (Bug #15675)

References: See also: Bug #15402.
- **MySQL Cluster:** Under some circumstances, it was possible for a restarting node to undergo a forced shutdown. (Bug #15632)
- **MySQL Cluster:** A node which failed during cluster startup was sometimes not removed from the internal list of active nodes. (Bug #15587)
- **Replication:** A replication slave server could sometimes crash on a `BEFORE UPDATE` trigger if the `UPDATE` query was not executed in the same database as the table with the trigger. (Bug #14614)
- When a connection using yaSSL was aborted, the server would continue to try to read the closed socket, and the thread continued to appear in the output of `SHOW PROCESSLIST`. Note that this issue did not affect secure connection attempts using OpenSSL. (Bug #15772)
- API function `mysql_stmt_prepare()` returned wrong field length for TEXT columns. (Bug #15613)
- **InnoDB:** Having two tables in a parent-child relationship enforced by a foreign key where one table used `ROW_FORMAT=COMPACT` and the other used `ROW_FORMAT=REDUNDANT` could result in a MySQL server crash. Note that this problem did not exist prior to MySQL 5.0.3, when the compact row format for `InnoDB` was introduced. (Bug #15550)
- **BDB:** A `DELETE`, `INSERT`, or `UPDATE` of a `BDB` table could cause the server to crash where the query contained a subquery using an index read. (Bug #15536)
- Resolution of the argument to the `VALUES()` function to a variable inside a stored routine caused a server crash. The argument must be a table column. (Bug #15441)
- A left join on a column that having a `NULL` value could cause the server to crash. (Bug #15268)
- The output of `mysqldump --triggers` did not contain the `DEFINER` clause in dumped trigger definitions. (Bug #15110)

- Reversing the order of operands in a `WHERE` clause testing a simple equality (such as `WHERE t1.col1 = t2.col2`) would produce different output from `EXPLAIN`. (Bug #15106)
- The output of `SHOW TRIGGERS` contained extraneous whitespace. (Bug #15103)
- Creating a trigger caused a server crash if the table or trigger database was not known because no default database had been selected. (Bug #14863)
- Column aliases were displayed incorrectly in a `SELECT` from a view following an update to a base table of the view. (Bug #14861)
- `SHOW [FULL] COLUMNS` and `SHOW INDEX` did not function with temporary tables. (Bug #14387, Bug #15224)
- The `INFORMATION_SCHEMA.COLUMNS` table did not report the size of `BINARY` or `VARBINARY` columns. (Bug #14271)
- `InnoDB`: If `foreign_key_checks` was 0, `InnoDB` permitted inconsistent foreign keys to be created. (Bug #13778)
- The server would not compile under Cygwin. (Bug #13640)
- `DESCRIBE` did not function with temporary tables. (Bug #12770)
- Set functions could not be aggregated in outer subqueries. (Bug #12762)
- A race condition when creating temporary files caused a deadlock on Windows with threads in `Opening tables` or `Waiting for table` states. (Bug #12071)

Changes in MySQL 5.0.17 (2005-12-14)

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- **Replication:** The syntax for `CREATE TRIGGER` now includes a `DEFINER` clause for specifying which access privileges to check at trigger invocation time. See [CREATE TRIGGER Syntax](#), for more information.

Known issue. If you attempt to replicate from a master server older than MySQL 5.0.17 to a slave running MySQL 5.0.17 through 5.0.19, replication of `CREATE TRIGGER` statements fails on the slave with a `Definer not fully qualified error`. A workaround is to create triggers on the master using a version-specific comment embedded in each `CREATE TRIGGER` statement:

```
CREATE /*!50017 DEFINER = 'root'@'localhost' */ TRIGGER ... ;
```

`CREATE TRIGGER` statements written this way will replicate to newer slaves, which pick up the `DEFINER` clause from the comment and execute successfully.

(Bug #16266)

- Support files for compiling with Visual Studio 6 have been removed. (Bug #15094)
- In the `latin5_turkish_ci` collation, the order of the characters `A WITH CIRCUMFLEX`, `I WITH CIRCUMFLEX`, and `U WITH CIRCUMFLEX` was changed. If you have used these characters in any indexed columns, you should rebuild those indexes. (Bug #13421)

- Recursion is permitted in stored procedures. Recursive stored functions and triggers still are not permitted. (Bug #10100)
- Added a `DEFINER` column to the `INFORMATION_SCHEMA.TRIGGERS` table.
- Invoking a stored function or trigger creates a new savepoint level. When the function or trigger finishes, the previous savepoint level is restored.

References: See also: Bug #13825.

- The maximum key length for `InnoDB` indexes was increased from 1024 bytes to 3072 bytes for all builds. (In MySQL 5.0.15, the length was increased but only for 64-bit builds.)
- Added the `SHOW FUNCTION CODE` and `SHOW PROCEDURE CODE` statements (available only for servers that have been built with debugging support). See [SHOW PROCEDURE CODE Syntax](#).

Bugs Fixed

- **MySQL Cluster:** A forced cluster shutdown occurred when the management daemon was restarted with a changed `config.ini` file that added an API or SQL node. (Bug #15512)
- **MySQL Cluster:** There was a small window for a node failure to occur during a backup without an error being reported. (Bug #15425)
- **MySQL Cluster:** Using `ORDER BY primary_key_column` when selecting from a table having the primary key on a `VARCHAR` column caused a forced shutdown of the cluster. (Bug #15240, Bug #15682, Bug #14828, Bug #15517)
- **MySQL Cluster:** Under certain circumstances, when `mysqld` connected to a cluster management server, the connection would fail before a node ID could be allocated. (Bug #15215)
- **MySQL Cluster:** Creating a table with packed keys failed silently. `NDB` now supports the `PACK_KEYS` option to `CREATE TABLE` correctly. (Bug #14514)
- **MySQL Cluster:** `REPLACE` failed when attempting to update a primary key value in a Cluster table. (Bug #14007)
- **Replication:** Stored functions making use of cursors were not replicated. (Bug #14077)
- **Replication:** On Windows, the server could crash during shutdown if both replication threads and normal client connection threads were active. (Bug #11796)
- **Replication: InnoDB:** During replication, There was a failure to record events in the binary log that still occurred even in the event of a `ROLLBACK`. For example, this sequence of commands:

```
BEGIN;
CREATE TEMPORARY TABLE t1 (a INT) ENGINE=INNODB;
ROLLBACK;
INSERT INTO t1 VALUES (1);
```

would succeed on the replication master as expected. However, the `INSERT` failed on the slave because the `ROLLBACK` would (erroneously) cause the `CREATE TEMPORARY TABLE` statement not to be written to the binlog. (Bug #7947)

- Corrected an error-handling problem within stored routines on 64-bit platforms. (Bug #15630)
- Slave SQL thread cleanup was not handled properly on Mac OS X when a statement was killed, resulting in a slave crash. (Bug #15623, Bug #15668)

- The `CREATE` test case in `mysql-test-run.pl` failed on AIX and SCO. (Bug #15607)
- A bug in `mysql-test/t/mysqltest.test` caused that test to fail. (Bug #15605)
- A statement that produced a warning, when fetched using `mysql_stmt_fetch()`, did not produce a warning count according to `mysql_warning_count()`. (Bug #15510)
- The database-changing code for stored routine handling caused an error-handling problem resulting in a server crash. (Bug #15392)
- The original Linux RPM packages (5.0.17-0) had an issue with a `zlib` dependency that would result in an error during an install or upgrade. They were replaced by new binaries, 5.0.17-1. Here is a list of the new RPM binaries:
 - `MySQL-{Max,client,devel,server,shared,ndb*}-5.0.17-1.i386.rpm`
 - `MySQL-*-standard-5.0.17-1.rhel3.i386.rpm`, `MySQL-*-standard-5.0.17-1.rhel3.ia64.rpm`, `MySQL-*-standard-5.0.17-1.rhel3.x86_64.rpm`
 - `MySQL-*-pro-5.0.17-1.rhel3.i386.rpm`, `MySQL-*-pro-5.0.17-1.rhel3.ia64.rpm`, `MySQL-*-pro-5.0.17-1.rhel3.x86_64.rpm`
 - `MySQL-*-pro-gpl-5.0.17-1.rhel3.i386.rpm`, `MySQL-*-pro-gpl-5.0.17-1.rhel3.ia64.rpm`, `MySQL-*-pro-gpl-5.0.17-1.rhel3.x86_64.rpm`
 (Bug #15223)
- `mysqld` would not start on Windows 9X operating systems including Windows Me. (Bug #15209)
- Queries that select records based on comparisons to a set of column could crash the server if there was one index covering the columns, and a set of other noncovering indexes that taken together cover the columns. (Bug #15204)
- Selecting from a view processed with the temptable algorithm caused a server crash if the query cache was enabled. (Bug #15119)
- `mysql --help` was missing a newline after the version string when the bundled `readline` library was not used. (Bug #15097)
- Creating a view that referenced a stored function that selected from a view caused a crash upon selection from the view. (Bug #15096)
- The server crashed if compiled without any transactional storage engines. (Bug #15047)
- Multiple-table update operations were counting updates and not updated rows. As a result, if a row had several updates it was counted several times for the “rows matched” value but updated only once. (Bug #15028)
- Symbolic links did not function properly on Windows platforms. (Bug #14960, Bug #14310)
- `ROW_COUNT()` returned an incorrect result after `EXECUTE` of a prepared statement. (Bug #14956)
- When using an aggregate function to select from a table that has a multiple-column primary key, adding `ORDER BY` to the query could produce an incorrect result. (Bug #14920)
- `ANALYZE TABLE` did not properly update table statistics for a `MyISAM` table with a `FULLTEXT` index containing stopwords, so a subsequent `ANALYZE TABLE` would not recognize the table as having already been analyzed. (Bug #14902)

- Creating a view within a stored procedure could result in an out of memory error or a server crash. (Bug #14885)
- `GROUP BY` on a view column did not correctly account for the possibility that the column could contain `NULL` values. (Bug #14850)
- The `mysql_stmt_fetch()` C API function could return `MYSQL_NO_DATA` for a `SELECT COUNT(*) FROM tbl_name WHERE 1 = 0` statement, which should return 1 row. (Bug #14845)
- Selecting from a view used `filesort` retrieval when faster retrieval was possible. (Bug #14816)
- `InnoDB`: A race condition permitted two threads to drop a hash index simultaneously. (Bug #14747)
- `SHOW CREATE TABLE` for a view could fail if the client had locked the view. (Bug #14726)
- The grammar for supporting the `DEFINER = CURRENT_USER` clause in `CREATE VIEW` and `ALTER VIEW` was incorrect. (Bug #14719)
- `ALTER TABLE ... SET DEFAULT` had no effect. (Bug #14693)
- Using `ORDER BY` on a column from a view, when also selecting the column normally, and through an alias, caused a mistaken `Column 'x' in order clause is ambiguous` error. (Bug #14662)
- `SELECT` queries that began with an opening parenthesis were not being placed in the query cache. (Bug #14652)
- In a stored procedure, continuing (via a condition handler) after a failed variable initialization caused a server crash. (Bug #14643)
- A `LIMIT`-related optimization failed to take into account that `MyISAM` table indexes can be disabled, causing Error 124 when it tried to use such an index. (Bug #14616)
- `mysqlhotcopy` tried to copy `INFORMATION_SCHEMA` tables. (Bug #14610)
- A server crash resulted from the following sequence of events: 1) With no default database selected, create a stored procedure with the procedure name explicitly qualified with a database name (`CREATE PROCEDURE db_name.proc_name ...`). 2) Create another stored procedure with no database name qualifier. 3) Execute `SHOW PROCEDURE STATUS`. (Bug #14569)
- `mysqldump --triggers` did not account for the SQL mode and could dump trigger definitions with missing whitespace if the `IGNORE_SPACE` mode was enabled. (Bug #14554)
- `CREATE TABLE tbl_name (...) SELECT ...` could crash the server and write invalid data into the `.frm` file if the `CREATE TABLE` and `SELECT` both contained a column with the same name. Also, if a default value is specified in the column definition, it is now actually used. (Bug #14480)
- The value of `INFORMATION_SCHEMA.TABLES.TABLE_TYPE` sometimes was reported as empty. (Bug #14476)
- `mysql_fix_privilege_tables.sql` contained an erroneous comment that resulted in an error when the file contents were processed. (Bug #14469)
- Queries on `ARCHIVE` tables that used the `filesort` sorting method could result in a server crash. (Bug #14433)
- Creating a table containing an `ENUM` or `SET` column from within a stored procedure or prepared statement caused a server crash later when executing the procedure or statement. (Bug #14410)
- For a table that had been opened with `HANDLER OPEN`, issuing `OPTIMIZE TABLE`, `ALTER TABLE`, or `REPAIR TABLE` caused a server crash. (Bug #14397)

- Declaring a stored routine variable to have a `DEFAULT` value that referred to a variable of the same name caused a server crash. (For example: `DECLARE x INT DEFAULT x`) Now the `DEFAULT` variable is interpreted as referring to a variable in an outer scope, if there is one. (Bug #14376)
- Complex subqueries could cause improper internal query execution environment initialization and crash the server. (Bug #14342)
- Within a stored procedure, inserting with `INSERT ... SELECT` into a table with an `AUTO_INCREMENT` column did not generate the correct sequence number. (Bug #14304)
- Space truncation was being ignored when inserting into `BINARY` or `VARBINARY` columns. Now space truncation results in a warning, or an error in strict mode. (Bug #14299)
- Casting a `FLOAT` or `DOUBLE` whose value was less than `1.0E-06` to `DECIMAL` would yield an inappropriate value. (Bug #14268)
- `CAST(expr AS BINARY(N))` did not pad with `0x00` to a length of `N` bytes. (Bug #14255)
- Manual manipulation of the `mysql.proc` table could cause a server crash. This should not happen, but it is also not supported that the server will notice such changes. (Bug #14233)
- A `UNION` of `DECIMAL` columns could produce incorrect results. (Bug #14216)
- The maximum value of `MAX_ROWS` was handled incorrectly on 64-bit systems. (Bug #14155)
- `CHAR(... USING ...)` and `CONVERT(CHAR(...) USING ...)`, though logically equivalent, could produce different results. (Bug #14146)
- The server could misinterpret old trigger definition files created before MySQL 5.0.17. Now they are interpreted correctly, but this takes more time and the server issues a warning that the trigger should be re-created. (Bug #14090)
- For an invalid view definition, selecting from the `INFORMATION_SCHEMA.VIEWS` table or using `SHOW CREATE VIEW` failed, making it difficult to determine what part of the definition was invalid. Now the server returns the definition and issues a warning. (Bug #13818)
- `InnoDB`: Activity on an `InnoDB` table caused execution time for `SHOW CREATE TABLE` for the table to increase. (Bug #13762)
- Within a stored procedure, exception handling for `UPDATE` statements that caused a duplicate-key error caused a `Packets out of order` error for the following statement. (Bug #13729)
- Statements that implicitly commit a transaction are prohibited in stored functions and triggers. An attempt to create a function or trigger containing such a statement produces an error. (The originally reported symptom was that a trigger that dropped another trigger could cause a server crash. That problem was fixed by the patch for Bug #13343.) (Bug #13627)

References: See also: Bug #13343.

- A newline character in a column alias in a view definition caused an error when selecting from the view later. (Bug #13622)
- Invoking a stored procedure within another stored procedure caused the server to crash. (Bug #13549)
- Warnings from a previous command were not being reset when fetching from a cursor. (Bug #13524)
- In some cases, a left outer join could yield an invalid result or cause the server to crash, due to a `MYSQL_DATA_TRUNCATED` error. (Bug #13488)

- `DELETE` from `CSV` tables reported an incorrect rows-affected value. (Bug #13406)
- A server crash could occur if a prepared statement updated a table for which a trigger existed when the statement was prepared but had been dropped prior to statement execution. (Bug #13399)
- `RESET MASTER` failed to delete log files on Windows. One consequence of this change is that server opens the general query and slow log files in shared mode, so now they can be renamed while the server has them open (something not true in previous versions). (Bug #13377)
- For binary string data types, `mysqldump --hex-blob` produced an illegal output value of `0x` rather than `' '`. (Bug #13318)
- `REPAIR TABLE`, `BACKUP TABLE`, `RESTORE TABLE` within a stored procedure caused a server crash. (Bug #13012)
- Implicit versus explicit conversion of float to integer (such as inserting a float value into an integer column versus using `CAST(... AS UNSIGNED)` before inserting the value) could produce different results. Implicit and explicit typecasts now are done the same way, with a value equal to the nearest integer according to the prevailing rounding mode. (Bug #12956)
- Some comparisons for the `IN()` operator were inconsistent with equivalent comparisons for the `=` operator. (Bug #12612)
- A server crash could occur if a prepared statement invoked a stored procedure that existed when the statement was prepared but had been dropped and re-created prior to statement execution. (Bug #12329)
- `make` failed when attempting to build MySQL in different directory other than that containing the source. (Bug #11827)
- Revised table locking to permit proper assessment of view security. (Bug #11555)
- Perform character set conversion of constant values whenever possible without data loss. (Bug #10446)
- Within a trigger definition the `CURRENT_USER()` function evaluated to the user whose actions caused the trigger to be activated. Now that triggers have a `DEFINER` value, `CURRENT_USER()` evaluates to the trigger definer. (Bug #5861)
- `mysql` ignored the `MYSQL_TCP_PORT` environment variable. (Bug #5792)

Changes in MySQL 5.0.16 (2005-11-10)

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- **MySQL Cluster:** The `InnoDB`, `NDB`, `BDB`, and `ARCHIVE` storage engines now support spatial columns. See [Extensions for Spatial Data](#).
- **Replication:** Added a `--hexdump` option to `mysqlbinlog` that displays a hex dump of the log in comments. This output can be helpful for replication debugging.
- When a date column is set `NOT NULL` and contains `0000-00-00`, it will be updated for `UPDATE` statements that contains `columnname IS NULL` in the `WHERE` clause. (Bug #14186)
- When trying to run the server with `yaSSL` enabled, MySQL now tries to open `/dev/random` automatically if `/dev/urandom` is not available. (Bug #13164)

- MySQL now supports character set conversion for seven additional `cp950` characters into the `big5` character set: `0xF9D6`, `0xF9D7`, `0xF9D8`, `0xF9D9`, `0xF9DA`, `0xF9DB`, and `0xF9DC`.

**Note**

If you move data containing these additional characters to an older MySQL installation which does not support them, you may encounter errors.

(Bug #12476)

- You must now declare a prefix for an index on any column of any `Geometry` class, the only exception being when the column is a `POINT`. (Bug #12267)
- The `read_only` system variable no longer applies to `TEMPORARY` tables. (Bug #4544)
- Due to changes in binary logging, the restrictions on which stored routine creators can be trusted not to create unsafe routines have been lifted for stored procedures (but not stored functions). Consequently, the `log_bin_trust_routine_creators` system variable and the corresponding `--log-bin-trust-routine-creators` server option were renamed to `log_bin_trust_function_creators` and `--log-bin-trust-function-creators`. For backward compatibility, the old names are recognized but result in a warning. See [Binary Logging of Stored Programs](#).
- The `CHECK TABLE` statement now works for `ARCHIVE` tables.
- In MySQL 5.0.13, syntax for `DEFINER` and `SQL SECURITY` clauses was added to the `CREATE VIEW` and `ALTER VIEW` statements, but the clauses had no effect. They now are enabled. They specify the security context to be used when checking access privileges at view invocation time. See [CREATE VIEW Syntax](#), for more information.
- Added the `Compression` status variable, which indicates whether the client connection uses compression in the client/server protocol.

Bugs Fixed

- **MySQL Cluster:** Repeated transactions using unique index lookups could cause a memory leak leading to error 288, `Out of index operations in transaction coordinator`. (Bug #14199)
- **MySQL Cluster:** A memory leak occurred when performing ordered index scans using indexes on columns larger than 32 bytes. This would eventually lead to the forced shutdown of all `mysqld` server processes used with the cluster. (Bug #13078)
- For some stored functions dumped by `mysqldump --routines`, the function definition could not be reloaded later due to a parsing error. (Bug #14723)
- Deletes from a `CSV` table could cause table corruption. (Bug #14672)
- Executing `REPAIR TABLE`, `ANALYZE TABLE`, or `OPTIMIZE TABLE` on a view for which an underlying table had been dropped caused a server crash. (Bug #14540)
- `mysqlmanager` did not start up correctly on Windows 2003. (Bug #14537)
- Selecting from a table in both an outer query and a subquery could cause a server crash. (Bug #14482)
- `ORDER BY DESC` within the `GROUP_CONCAT()` function was not honored when used in a view. (Bug #14466)
- The input polling loop for Instance Manager did not sleep properly. Instance Manager used up too much CPU as a result. (Bug #14388)

- Indexes for `BDB` tables were being limited incorrectly to 255 bytes. (Bug #14381)
- The `mysql` parser did not properly strip the delimiter from input lines less than nine characters long. For example, this could cause `USE abc;` to result in an `Unknown database: abc;` error. (Bug #14358)
- The displayed value for the `CHARACTER_MAXIMUM_LENGTH` column in the `INFORMATION_SCHEMA.COLUMNS` table was not adjusted for multibyte character sets. (Bug #14290)
- The parser did not correctly recognize wildcards in the host part of the `DEFINER` user in `CREATE VIEW` statements. (Bug #14256)
- Memory corruption and a server crash could be caused by statements that used a cursor and generated a result set larger than `max_heap_table_size`. (Bug #14210)
- A bug fix in MySQL 5.0.15 caused the displayed values for the `CHARACTER_MAXIMUM_LENGTH` and `CHARACTER_OCTET_LENGTH` columns in the `INFORMATION_SCHEMA.COLUMNS` table to be reversed. (Bug #14207)
- Statements of the form `CREATE TABLE ... SELECT ...` that created a column with a multibyte character set could incorrectly calculate the maximum length of the column, resulting in a `Specified key was too long` error. (Bug #14139)
- Use of `WITH ROLLUP PROCEDURE ANALYSE()` could hang the server. (Bug #14138)
- On Windows, the value of `character_sets_dir` in `SHOW VARIABLES` output was displayed inconsistently (using both `/"` and `\"` as path name component separators). (Bug #14137)
- A comparison with an invalid date (such as `WHERE col_name > '2005-09-31'`) caused any index on `col_name` not to be used and a string comparison for each row, resulting in slow performance. (Bug #14093)
- Subqueries in the `FROM` clause failed if the current database was `INFORMATION_SCHEMA`. (Bug #14089)
- For `InnoDB` tables, using a column prefix for a `utf8` column in a primary key caused `Cannot find record` errors when attempting to locate records. (Bug #14056)
- Some updatable views could not be updated. (Bug #14027)
- A prepared statement that selected from a view processed using the merge algorithm could crash on the second execution. (Bug #14026)
- When the `DATE_FORMAT()` function appeared in both the `SELECT` and `ORDER BY` clauses of a query but with arguments that differ by case (for example, `%m` and `%M`), incorrect sorting may have occurred. (Bug #14016)
- `TIMEDIFF()`, `ADDTIME()`, and `STR_TO_DATE()` were not reporting that they could return `NULL`, so functions that invoked them might misinterpret their results. (Bug #14009)
- Within stored routines, `REPLACE()` could return an empty string (rather than the original string) when no replacement was done, and `IFNULL()` could return garbage results. (Bug #13941)
- Inserting a new row into an `InnoDB` table could cause `DATETIME` values already stored in the table to change. (Bug #13900)
- An update of a `CSV` table could cause a server crash. (Bug #13894)
- Corrected a parser precedence problem that resulted in an `Unknown column ... in 'on clause'` error for some joins. (Bug #13832)

- Trying to take the logarithm of a negative value is now handled in the same fashion as division by zero. That is, it produces a warning when `ERROR_FOR_DIVISION_BY_ZERO` is set, and an error in strict mode. (Bug #13820)
- The example configuration files supplied with MySQL distributions listed the `thread_cache_size` variable as `thread_cache`. (Bug #13811)
- `mysqld_safe` did not correctly start the `-max` version of the server (if it was present) if the `--ledir` option was given. (Bug #13774)
- `SHOW CREATE TABLE` did not display the `CONNECTION` string for `FEDERATED` tables. (Bug #13724)
- For a `MyISAM` table originally created in MySQL 4.1, `INSERT DELAYED` could cause a server crash. (Bug #13707)
- The server incorrectly accepted column definitions of the form `DECIMAL(0,D)` for `D` less than 11. (Bug #13667)
- Trying to create a stored routine with no database selected would crash the server. (Bug #13587, Bug #13514)
- Inserts of too-large `DECIMAL` values were handled inconsistently (sometimes set to the maximum `DECIMAL` value, sometimes set to 0). (Bug #13573)
- `TIMESTAMPDIFF()` returned an incorrect result if one argument but not the other was a leap year and a date was from March or later. (Bug #13534)
- Specifying `--default-character-set=cp-932` for `mysqld` would cause SQL scripts containing comments written using that character set to fail with a syntax error. (Bug #13487)
- Use of `col_name = VALUES(col_name)` in the `ON DUPLICATE KEY UPDATE` clause of an `INSERT` statement failed with an `Column 'col_name' in field list is ambiguous` error. (Bug #13392)
- The default value of `query_prealloc_size` was set to 8192, lower than its minimum of 16384. The minimum has been lowered to 8192. (Bug #13334)
- `InnoDB`: When dropping and adding a `PRIMARY KEY`, if a loose index scan using only the second part of multiple-part index was chosen, incorrect keys were created and an endless loop resulted. (Bug #13293)
- `mysqladmin` and `mysqldump` would hang on SCO OpenServer. (Bug #13238)
- `SELECT DISTINCT CHAR(col_name)` returned incorrect results after `SET NAMES utf8`. (Bug #13233)
- For queries with nested outer joins, the optimizer could choose join orders that query execution could not handle. The fix is that now the optimizer avoids choosing such join orders. (Bug #13126)
- The server did not take character set into account in checking the width of the `mysql.user.Password` column. As a result, it could incorrectly generate long password hashes even if the column was not long enough to hold them. (Bug #13064)
- The source distribution failed to compile when configured with the `--without-geometry` option. (Bug #12991)
- Use of the deprecated `--sql-bin-update-same` option caused a server crash. (Bug #12974)
- Maximum values were handled incorrectly for command-line options of type `GET_LL`. (Bug #12925)
- `mysqldump` could not dump views if the `-x` option was given. (Bug #12838)

- Two threads that were creating triggers on an `InnoDB` table at the same time could deadlock. (Bug #12739)
- `InnoDB`: Large `innobase_buffer_pool_size` and `innobase_log_file_size` values were displayed incorrectly on 64-bit systems. (Bug #12701)
- For `LIKE ... ESCAPE`, an escape sequence longer than one character was accepted as valid. Now the sequence must be empty or one character long. If the `NO_BACKSLASH_ESCAPES` SQL mode is enabled, the sequence must be one character long. (Bug #12595)
- Inserting `cp932` strings into a `VARCHAR` column caused a server crash rather than string truncation if the string was longer than the column definition. (Bug #12547)
- A prepared statement failed with `Illegal mix of collations` if the client character set was `utf8` and the statement used a table that had a character set of `latin1`. (Bug #12371)
- Using `ALTER TABLE` to add an index could fail if the operation ran out of temporary file space. Now it automatically makes a second attempt that uses a slower method but no temporary file. In this case, problems that occurred during the first attempt can be displayed with `SHOW WARNINGS`. (Bug #12166)
- `mysqlimport` now issues a `SET @@character_set_database = binary` statement before loading data so that a file containing mixed character sets (columns with different character sets) can be loaded properly. (Bug #12123)
- Running `OPTIMIZE TABLE` and other data-updating statements concurrently on an `InnoDB` table could cause a crash or the following warnings in the error log: `Warning: Found locks from different threads in write: enter write_lock,Warning: Found locks from different threads in write: start of release lock`. (Bug #11704)
- `LOAD DATA INFILE` would not accept the same character for both the `ESCAPED BY` and the `ENCLOSED BY` clauses. (Bug #11203)
- The value of `Last_query_cost` was not updated for queries served from the query cache. (Bug #10303)
- Starting `mysqld` with the `--skip-innodb` and `--default-storage-engine=innodb` (or `--default-table-type=innodb`) caused a server crash. (Bug #9815)
- The `--exit-info=65536` option conflicted with `--temp-pool` and caused problems with the server's use of temporary files. Now `--temp-pool` is ignored if `--exit-info=65536` is specified. (Bug #9551)
- For a user that has the `SELECT` privilege on a view, the server erroneously was also requiring the user to have the `EXECUTE` privilege at view execution time for stored functions used in the view definition. (Bug #9505)
- Where one stored procedure called another stored procedure: If the second stored procedure generated an exception, the exception was not caught by the calling stored procedure. For example, if stored procedure `A` used an `EXIT` statement to handle an exception, subsequent statements in `A` would be executed regardless when `A` was called by another stored procedure `B`, even if an exception that should have been handled by the `EXIT` was generated in `A`. (Bug #7049)
- On Windows, the server was not ignoring hidden or system directories that Windows may have created in the data directory, and would treat them as available databases. (Bug #4375)

Changes in MySQL 5.0.15 (2005-10-19, Production)

- [Functionality Added or Changed](#)

- [Bugs Fixed](#)

Functionality Added or Changed

- **Incompatible Change:** For `BINARY` columns, the pad value and how it is handled has changed. The pad value for inserts now is `0x00` rather than space, and there is no stripping of the pad value for selects. For details, see [The BINARY and VARBINARY Types](#).
- **Incompatible Change:** The `CHAR()` function now returns a binary string rather than a string in the connection character set. An optional `USING charset` clause may be used to produce a result in a specific character set instead. Also, arguments larger than 256 produce multiple characters. They are no longer interpreted modulo 256 to produce a single character each. These changes may cause some incompatibilities, as noted in [Changes Affecting Upgrades to 5.0](#).
- **MySQL Cluster:** The `ndb_mgm` client now reports node startup phases automatically. (Bug #16197)
- **MySQL Cluster:** A new “smart” node allocation algorithm means that it is no longer necessary to use sequential IDs for cluster nodes, and that nodes not explicitly assigned IDs should now have IDs allocated automatically in most cases. In practical terms, this means that it is now possible to assign a set of node IDs such as `1, 2, 4, 5` without an error being generated due to the missing `3`. (Bug #13009)
- **MySQL Cluster:** A number of new or improved error messages have been implemented in this release to provide better and more accurate diagnostic information regarding cluster configuration issues and problems. (Bug #12786, Bug #11749, Bug #13197, Bug #11739, Bug #12044)
- The following statements now cause an implicit `COMMIT`:
 - `CREATE VIEW`
 - `ALTER VIEW`
 - `DROP VIEW`
 - `CREATE TRIGGER`
 - `DROP TRIGGER`
 - `CREATE USER`
 - `RENAME USER`
 - `DROP USER`(Bug #13343)
- Added the `--tz-utc` option to `mysqldump`. This option adds `SET TIME_ZONE='+00:00'` to the dump file so that `TIMESTAMP` columns can be dumped and reloaded between servers in different time zones and protected from changes due to daylight saving time. (Bug #13052)
- When executing single-table `UPDATE` or `DELETE` queries containing an `ORDER BY ... LIMIT N` clause, but not having any `WHERE` clause, MySQL can now take advantage of an index to read the first `N` rows in the ordering specified in the query. If an index is used, only the first `N` records will be read, as opposed to scanning the entire table. (Bug #12915)
- The `MySQL-server` RPM now explicitly assigns the `mysql` system user to the `mysql` user group during the postinstallation process. This corrects an issue with upgrading the server on some Linux distributions whereby a previously existing `mysql` user was not changed to the `mysql` group, resulting in wrong groups for files created following the installation. (Bug #12823)

- The maximum key length for `InnoDB` indexes was increased from 1024 bytes to 3072 bytes for 64-bit builds.
- When declaring a local variable (or parameter) named `password` or `name`, and setting it with `SET` (for example, `SET password = ''`), the new error message `ERROR 42000: Variable 'nnn' must be quoted with `...`, or renamed` is returned (where 'nnn' is 'password' or 'names'). This means there is a syntax conflict with special sentences like `SET PASSWORD = PASSWORD(...)` (for setting a user's password) and `set names default` (for setting charset and collation).

This must be resolved either by quoting the variable name: `SET `password` = ...`, which will set the local variable ``password``, or by renaming the variable to something else (if setting the user's password is the desired effect).

Bugs Fixed

- **MySQL Cluster:** The `pererror` utility included with the `MySQL-Server` RPM did not provide support for the `--ndb` option. It now supports this option, and so can be used to obtain error message text for MySQL Cluster error codes. (Bug #13740)
- **MySQL Cluster:** Placing multiple `[tcp default]` sections in the cluster's `config.ini` file crashed `ndb_mgmd`. (The process now exits gracefully in such cases, with an appropriate error message.) (Bug #13611)
- **MySQL Cluster:** `ndb_mgmd` permitted a node to be stopped or restarted while another node was still starting up, which could crash the cluster. It should now not be possible to issue a node stop or restart while a different node is still restarting, and the cluster management client should issue an error when such an attempt is made. (Bug #13461)
- **MySQL Cluster:** Trying to run `ndbd` as system `root` when connecting to a `mysqld` process running as the `mysql` system user using SHM caused the `ndbd` process to crash. (`ndbd` should now exit gracefully with an appropriate error message instead.) (Bug #9249)
- **Replication:** An `UPDATE` query using a join would be executed incorrectly on a replication slave. (Bug #12618)
- Tests containing `SHOW TABLE STATUS` or `INFORMATION_SCHEMA` failed on `opnsrv6c`. (Bug #14064, Bug #14065)
- `mysqldump` could not dump views. (Bug #14061)
- `mysqlcheck --all-databases --analyze --optimize` failed because it also tried to analyze and optimize the `INFORMATION_SCHEMA` tables which it can't. (Bug #13783)
- Character set conversion was not being done for `FIND_IN_SET()`. (Bug #13751)
- On BSD systems, the system `crypt()` call could return an error for some salt values. The error was not handled, resulting in a server crash. (Bug #13619)
- When calling a stored procedure with the syntax `CALL schema.procedurename` and no default schema selected, `ERROR 1046` was displayed after the procedure returned. (Bug #13616)
- A column in the `ON` condition of a join that referenced a table in a nested join could not be resolved if the nested join was a right join. (Bug #13597)
- The server could over-allocate memory when performing a `FULLTEXT` search for stopwords only. (Bug #13582)
- `CREATE DEFINER=... VIEW ...` caused the server to crash when run with `--skip-grant-tables`. (Bug #13504)

- **InnoDB**: Queries that were executed using an `index_merge` union or intersection could produce incorrect results if the underlying table used the **InnoDB** storage engine and had a primary key containing `VARCHAR` members. (Bug #13484)
- A qualified reference to a view column in the `HAVING` clause could not be resolved. (Bug #13410)
- `CAST(1E+300 TO SIGNED INT)` produced an incorrect result on little-endian machines. (Bug #13344)
- Queries that use indexes in normal `SELECT` statements may cause range scans in `VIEWS`. (Bug #13327)
- `SELECT * INTO OUTFILE ... FROM INFORMATION_SCHEMA.schemata` failed with an `Access denied` error. (Bug #13202)
- `mysqldump --triggers` did not quote identifiers properly if the `--compatible` option was given, so the dump output could not be reloaded. (Bug #13146)
- A table or view named Ç (C-cedilla) couldn't be dropped. (Bug #13145)
- For XA transaction IDs (`gtrid.bqual.formatID`), uniqueness is supposed to be assessed based on `gtrid` and `bqual`. MySQL was also including `formatID` in the uniqueness check. (Bug #13143)
- Trying to create a view dynamically using a prepared statement within a stored procedure failed with error 1295. (Bug #13095)
- `comp_err` did not detect when multiple error messages for a language were given for an error symbol. (Bug #13071)
- If special characters such as `'_'`, `'%'`, or the escape character were included within the prefix of a column index, `LIKE` pattern matching on the indexed column did not return the correct result. (Bug #13046, Bug #13919)
- Using an undefined variable in an `IF` or `SET` statement inside a stored routine produced an incorrect `unknown column ... in 'order clause'` error message. (Bug #13037)
- With `--log-slave-updates Exec_master_log_pos` of SQL thread lagged IO (Bug #13023)
- `SHOW CREATE TABLE` did not display any `FOREIGN KEY` clauses if a temporary file could not be created. Now `SHOW CREATE TABLE` displays an error message in an SQL comment if this occurs. (Bug #13002)
- Local (non-XA) and XA transactions are supposed to be mutually exclusive within a given client connection, but this prohibition was not always enforced. (Bug #12935)
- Server crashed during a `SELECT` statement, writing a message like this to the error log:

```
InnoDB: Error: MySQL is trying to perform a SELECT
InnoDB: but it has not locked any tables in ::external_lock()!
```

(Bug #12736)

- An expression in an `ORDER BY` clause failed with `Unknown column 'col_name' in 'order clause'` if the expression referred to a column alias. (Bug #11694)
- Issuing `STOP SLAVE` after having acquired a global read lock with `FLUSH TABLES WITH READ LOCK` caused a deadlock. Now `STOP SLAVE` generates an error in such circumstances. (Bug #10942)
- Corrected a memory-copying problem for `big5` values when using `icc` compiler on Linux IA-64 systems. (Bug #10836)

- The `--interactive-timeout` and `--slave-net-timeout` options for `mysqld` were not being obeyed on Mac OS X and other BSD-based platforms. (Bug #8731)
- Queries of the form `(SELECT ...) ORDER BY ...` were being treated as a `UNION`. This improperly resulted in only distinct values being returned (because `UNION` by default eliminates duplicate results). Also, references to column aliases in `ORDER BY` clauses following parenthesized `SELECT` statements were not resolved properly. (Bug #7672)
- Character set file parsing during `mysql_real_connect()` read past the end of a memory buffer. (Bug #6413)

Changes in MySQL 5.0.14 (Not released)

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- **Replication:** Multiple-table `UPDATE` and `DELETE` statements that do not affect any rows are now written to the binary log and will replicate. (Bug #13348, Bug #12844)
- Range scans can now be performed for queries on VIEWS such as `column IN (<constants>)` and `column BETWEEN ConstantA AND ConstantB`. (Bug #13317)
- The limit of 255 characters on the input buffer for `mysql` on Windows has been lifted. The exact limit depends on what the system permits, but can be up to 64KB characters. A typical limit is 16KB characters. (Bug #12929)
- Added the `myisam_stats_method`, which controls whether `NULL` values in indexes are considered the same or different when collecting statistics for `MyISAM` tables. This influences the query optimizer as described in [MyISAM Index Statistics Collection](#). (Bug #12232)
- The `CHAR()` function now takes into account the character set and collation given by the `character_set_connection` and `collation_connection` system variables. For an argument `n` to `CHAR()`, the result is `n mod 256` for single-byte character sets. For multibyte character sets, `n` must be a valid code point in the character set. Also, the result string from `CHAR()` is checked for well-formedness. For invalid arguments, or a result that is not well-formed, MySQL generates a warning (or, in strict SQL mode, an error). (Bug #10504)
- Re-enabled the `--delayed-insert` option for `mysqldump`, which now checks for each table dumped whether its storage engine supports `DELAYED` inserts. (Bug #7815)
- `RENAME TABLE` now works for views as well, as long as you do not try to rename a view into a different database. (Bug #5508)
- Configure-time checking for the availability of multibyte macros and functions in the bundled `readline` library. This improves handling of multibyte character sets in the `mysql` client. (Bug #3982)
- When an `InnoDB` foreign key constraint is violated, the error message now indicates which table, column, and constraint names are involved. (Bug #3443)

Bugs Fixed

- **MySQL Cluster:** A trigger updating the value of an `AUTO_INCREMENT` column in an `NDB` table would insert an error code rather than the expected value into the column. (Bug #13961)
- **MySQL Cluster:** If `ndb_restore` could not find a free `mysqld` process, it crashed. (Bug #13512)

- **MySQL Cluster:** Adding an index to a table with a large number of columns (more than 100) crashed the storage node. (Bug #13316)
- **MySQL Cluster:** `BIT` columns and following columns in `NDB` tables were corrupt when dumped by `mysqldump`. (Bug #13152)
- **MySQL Cluster:** Queries on `NDB` tables that were executed using `index_merge` could produce incorrect results. (Bug #13081)
- **MySQL Cluster:** Receipt of several `ENTER SINGLE USER MODE` commands by multiple `ndb_mgmd` processes within a short period of time resulted in cluster shutdown. (Bug #13053)
- **MySQL Cluster:** Multiple `ndb_mgmd` processes in a cluster did not know each other's IP addresses. (Bug #12037)
- **MySQL Cluster:** With two `mgmd` processes in a cluster, `ndb_mgm` output for `SHOW` would display the same IP address for both processes, even when they were on different hosts. (Bug #11595)
- **MySQL Cluster:** `LOAD DATA INFILE` with a large data file failed. (Bug #10694)
- **MySQL Cluster:** When deleting a great many (tens of thousands of) rows at once from an `NDB` table, an improperly dereferenced pointer could cause the `mysqld` process to crash. (Bug #9282)
- **Replication:** The `--replicate-rewrite-db` and `--replicate-do-table` options did not work for statements in which tables were aliased to names other than those listed by the options. (Bug #11139)
- Certain joins using `Range checked for each record` in the query execution plan could cause the server to crash. (Bug #24776)
- Joins nested under `NATURAL` or `USING` joins were sometimes not initialized properly, causing a server crash. (Bug #13545)
- After running `configure` with the `--with-embedded-privilege-control` option, the embedded server failed to build. (Bug #13501)
- The optimizer chose a less efficient execution plan for `col_name BETWEEN const AND const` than for `col_name = const`, even though the two expressions are logically equivalent. Now the optimizer can use the `ref` access method for both expressions. (Bug #13455)
- Locking a view with the query cache enabled and `query_cache_wlock_invalidate` enabled could cause a server crash. (Bug #13424)
- A `HAVING` clause that references an unqualified view column name could crash the server. (Bug #13411)
- The `--skip-innodb-doublewrite` option disables use of the `InnoDB` doublewrite buffer. However, having this option in effect when creating a new MySQL installation prevented the buffer from even being created, resulting in a server crash later. (Bug #13367)
- Calling the `FORMAT()` function with a `DECIMAL` column value caused a server crash when the value was `NULL`. (Bug #13361)
- Comparisons involving row constructors containing constants could cause a server crash. (Bug #13356)
- Aggregate functions sometimes incorrectly were permitted in the `WHERE` clause of `UPDATE` and `DELETE` statements. (Bug #13180)
- `NATURAL` joins and joins with `USING` against a view could return `NULL` rather than the correct value. (Bug #13127)

- For queries with `DISTINCT` and `WITH ROLLUP`, the `DISTINCT` should be applied after the rollup operation, but was not always. (Bug #12887)
- It was possible to create a view that executed a stored function for which you did not have the `EXECUTE` privilege. (Bug #12812)
- Shared-memory connections were not working on Windows. (Bug #12723)
- The server was not rejecting `FLOAT(M,D)` or `DOUBLE(M,D)` columns specifications when `M` was less than `D`. (Bug #12694)
- `CHECKSUM TABLE` locked `InnoDB` tables and did not use a consistent read. (Bug #12669)
- Incorrect creation of `DECIMAL` local variables in a stored procedure could cause a server crash. (Bug #12589)
- For queries for which the optimizer determined a join type of “Range checked for each record” (as shown by `EXPLAIN`, the query sometimes could cause a server crash, depending on the data distribution. (Bug #12291)
- After running `configure` with the `--without-server` option, the distribution failed to build. (Bug #11680, Bug #13550)
- Use of a user-defined function within the `HAVING` clause of a query resulted in an `Unknown column` error. (Bug #11553)
- The server crashed when processing a view that invoked the `CONVERT_TZ()` function. (Bug #11416)
- When `SELECT ... FOR UPDATE` or `SELECT ... LOCK IN SHARE MODE` for an `InnoDB` table were executed from within a stored function or a trigger, they were converted to a nonlocking consistent read. (Bug #11238)
- Queries against a `MERGE` table that has a composite index could produce incorrect results. (Bug #9112)
- MySQL programs in binary distributions for Solaris 8/9/10 x86 systems would not run on Pentium III machines. (Bug #6772)
- Nested handlers within stored procedures didn't work. (Bug #6127)

Changes in MySQL 5.0.13 (2005-09-22, Release Candidate)

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- **Replication:** Better detection of connection timeout for replication servers on Windows enables elimination of extraneous `Lost connection` errors in the error log. (Bug #5588)
- `OPTIMIZE TABLE` and `HANDLER` now are prohibited in stored procedures and functions and in triggers. (Bug #12953, Bug #12995)
- The `LEAST()` and `GREATEST()` functions used to return `NULL` only if all arguments were `NULL`. Now they return `NULL` if any argument is `NULL`, the same as Oracle. (Bug #12791)
- `InnoDB:` The `TRUNCATE TABLE` statement for `InnoDB` tables always resets the counter for an `AUTO_INCREMENT` column now, regardless of whether there is a foreign key constraint on the table. (Beginning with 5.0.3, `TRUNCATE TABLE` reset the counter, but only if there was no such constraint.) (Bug #11946)

- Reorder network startup to come after all other initialization, particularly storage engine startup which can take a long time. This also prevents MySQL from being run on a privileged port (any port under 1024) unless run as the root user. (Bug #11707)
- The restriction on the use of `PREPARE`, `EXECUTE`, and `DEALLOCATE PREPARE` within stored procedures was lifted. The restriction still applies to stored functions and triggers. (Bug #10975, Bug #10605)

References: See also: Bug #7115.

- A new command line argument was added to `mysqld` to ignore client character set information sent during handshake, and use server side settings instead, to reproduce 4.0 behavior :

```
mysqld --skip-character-set-client-handshake
```

(Bug #9948)

- Added a `--routines` option for `mysqldump` that enables dumping of stored routines. (Bug #9056)
- `RAND()` no longer permits nonconstant initializers. (Previously, the effect of nonconstant initializers is undefined.) (Bug #6172)
- The syntax for `CREATE VIEW` and `ALTER VIEW` statements now includes `DEFINER` and `SQL SECURITY` clauses for specifying the security context to be used when checking access privileges at view invocation time. (The syntax is present in 5.0.13, but these clauses have no effect until 5.0.16.) See [CREATE VIEW Syntax](#), for more information.
- The `--hex-dump` option for `mysqldump` now also applies to `BIT` columns.
- Two new collations have been added for Esperanto: `utf8_esperanto_ci` and `ucs2_esperanto_ci`.
- The Windows binary packages are now compiled with the Microsoft Visual Studio 2003 compiler instead of Microsoft Visual C++ 6.0.
- The connection string for `FEDERATED` tables now is specified using a `CONNECTION` table option rather than a `COMMENT` table option.
- The binaries compiled with the Intel `icc` compiler are now built using `icc 9.0` instead of `icc 8.1`. You will have to install new versions of the Intel `icc` runtime libraries, which are available from here: <http://dev.mysql.com/downloads/os-linux.html>

Bugs Fixed

- **Incompatible Change:** A lock wait timeout caused `InnoDB` to roll back the entire current transaction. Now it rolls back only the most recent SQL statement. (Bug #12308)
- **MySQL Cluster:** The cluster management client `START BACKUP` command could be interrupted by a `SHOW` command. (Bug #13054)
- **MySQL Cluster:** A cluster shutdown following the crash of a data node failed to terminate any remaining node processes, even though `ndb_mgm` showed the shutdown request as having been completed. (Bug #9996, Bug #10938, Bug #11623)
- **MySQL Cluster:** The average row size for Cluster tables was calculated incorrectly. This affected the values shown for the `Data_length` and `Avg_row_length` columns in the output generated by `SHOW TABLE STATUS` as well as the values for the `data_length` and `data_length/table_rows` columns shown in the `TABLES` table of the `INFORMATION_SCHEMA` database with respect to Cluster tables.

Tables using storage engines other than `NDB` were not affected by this bug. (Bug #9896)

- **Replication:** Within a transaction, the following statements now cause an implicit commit: `CREATE FUNCTION`, `DROP FUNCTION`, `DROP PROCEDURE` (for stored functions, not UDFs), `ALTER FUNCTION`, `ALTER PROCEDURE`, `CREATE PROCEDURE`. This corrects a problem where these statements followed by `ROLLBACK` might not be replicated properly. (Bug #12870)
- **Replication:** Replication of `LOAD DATA INFILE` failed between systems using different path name syntax (such as delimiter characters). (Bug #11815)
- Local variables in stored routines were not always initialized correctly. (Bug #13133)
- The `FEDERATED` storage engine does not support `ALTER TABLE`, but no appropriate error message was issued. (Bug #13108)
- Columns named in the `USING()` clause of `JOIN ... USING()` were incorrectly resolved in case-sensitive fashion. (Bug #13067)
- For a server compiled with yaSSL, clients that used MySQL Connector/J were not able to establish SSH connections. (Bug #13029)
- When used in view definitions, `DAYNAME(expr)`, `DAYOFWEEK(expr)`, `WEEKDAY(expr)` were incorrectly treated as though the expression was `TO_DAYS(expr)` or `TO_DAYS(TO_DAYS(expr))`. (Bug #13000)
- Using `AS` to rename a column selected from a view in a subquery made it not possible to refer to that column in the outer query. (Bug #12993)
- Using an `INOUT` parameter with a `DECIMAL` data type in a stored procedure caused a server crash. (Bug #12979)
- `SELECT ... JOIN ... ON ... JOIN ... USING` caused a server crash. (Bug #12977)
- A bug introduced in MySQL 5.0.12 caused `SHOW TABLE STATUS` to display an `Auto_increment` value of 0 for `InnoDB` tables. (Bug #12973)
- On HP-UX 11.x (PA-RISC), the `-L` option caused `mysqlimport` to crash. (Bug #12958)
- `InnoDB`: A consistent read could return inconsistent results due to a bug introduced in MySQL 5.0.5. (Bug #12947)
- Incorrect implicit nesting of joins caused the parser to fail on queries of the form `SELECT ... FROM t1 JOIN t2 JOIN t3 ON t1.t1col = t3.t3col` with an `Unknown column 't1.t1col' in 'on clause'` error. (Bug #12943)
- Incorrect results could be returned from a view processed using a temporary table. (Bug #12941)
- Multiplying a `DECIMAL` value within a loop in a stored routine could incorrectly result in a value of `NULL`. (Bug #12938)
- Using `GROUP BY` when selecting from a view in some cases could cause incorrect results to be returned. (Bug #12922)
- The counters for the `Key_read_requests`, `Key_reads`, `Key_write_requests`, and `Key_writes` status variables were changed from `unsigned long` to `unsigned longlong` to accommodate larger values before the variables roll over and restart from 0. (Bug #12920)
- `mysql` and `mysqldump` were ignoring the `--defaults-extra-file` option. (Bug #12917)
- `SHOW FIELDS FROM schemaname.viewname` caused error 1046 when no default schema was set. (Bug #12905)

- `UNION [DISTINCT]` was not removing all duplicates for multibyte character values. (Bug #12891)
- A column that can be `NULL` was not handled properly for `WITH ROLLUP` in a subquery or view. (Bug #12885)
- `GROUP_CONCAT()` ignored an empty string if it was the first value to occur in the result. (Bug #12863)
- If a client has opened an `InnoDB` table for which the `.ibd` file is missing, `InnoDB` would not honor a `DROP TABLE` statement for the table. (Bug #12852)
- Within a stored procedure, a server crash was caused by assigning to a `VARCHAR INOUT` parameter the value of an expression that included the variable itself. (For example, `SET c = c.`) (Bug #12849)
- The server crashed when one thread resized the query cache while another thread was using it. (Bug #12848)
- A concurrency problem for `CREATE ... SELECT` could cause a server crash. (Bug #12845)
- `DO IFNULL(NULL, NULL)` and `SELECT CAST(IFNULL(NULL, NULL) AS DECIMAL)` caused a server crash. (Bug #12841)
- After changing the character set with `SET CHARACTER SET`, the result of the `GROUP_CONCAT()` function was not converted to the proper character set. (Bug #12829)
- The Windows installer made a change to one of the `mysql.proc` table files, causing stored routine functionality to be compromised. The Windows installer now never overwrites files in the MySQL data directory. During an upgrade from one version to another, a file in the data directory will not be overwritten even if it has not been modified since it was put there by an older installer.

If you have already lost access to stored routines because of this problem, you can get them back using the following procedure:

- Stop the server.
- In the `mysql\data` directory under your MySQL installation directory, and replace the `proc.frm` file with corresponding file from the version of MySQL that you were using before you upgraded.
- Start the server.
- Start the `mysql` command-line client (use the `root` account or another account that has full database privileges) and execute the `mysql_fix_privilege_tables.sql` script that upgrades the grant tables to the current structure. Instructions for doing this are given in [mysql_fix_privilege_tables — Upgrade MySQL System Tables](#).

After this, all stored routine functionality should work. (Bug #12820)

- Queries with subqueries, where the inner subquery uses the `range` or `index_merge` access method, could return incorrect results. (Bug #12720)
- The server failed to disallow `SET autocommit` in stored functions and triggers. It is permitted to change the value of `autocommit` in stored procedures, but a runtime error might occur if the procedure is invoked from a stored function or trigger. (Bug #12712)
- Simultaneous execution of DML statements and `CREATE TRIGGER` or `DROP TRIGGER` statements on the same table could cause server crashes or errors. (Bug #12704)
- Performing an `IS NULL` check on the `MIN()` or `MAX()` of an indexed column in a complex query could produce incorrect results. (Bug #12695)

- Use of `PREPARE` and `EXECUTE` with a statement that selected from a view in a subquery could cause a server crash. (Bug #12651)
- If the binary log is enabled, execution of a stored procedure that modifies table data and uses user variables could cause a server crash or incorrect information to be written to the binary log. (Bug #12637)
- The `LIKE ... ESCAPE` syntax produced invalid results when escape character was larger than one byte. (Bug #12611)
- `mysqldump` did not dump triggers properly. (Bug #12597)
- `InnoDB`: Limit recursion depth to 200 in deadlock detection to avoid running out of stack space. (Bug #12588)
- The `mysql.server` script contained an incorrect path for the `libexec` directory. (Bug #12550)
- A `UNION` of long `utf8 VARCHAR` columns was sometimes returned as a column with a `LONGTEXT` data type rather than `VARCHAR`. This could prevent such queries from working at all if selected into a `MEMORY` table because the `MEMORY` storage engine does not support the `TEXT` data types. (Bug #12537)
- A client connection thread cleanup problem caused the server to crash when closing the connection if the binary log was enabled. (Bug #12517)
- Use of the `mysql` client `HELP` command from within a stored routine caused a “packets out of order” error and a lost connection. Now `HELP` is detected and not permitted within stored routines. (Bug #12490)
- The `SYSDATE()` function now returns the time at which it was invoked. In particular, within a stored routine or trigger, `SYSDATE()` returns the time at which it executes, not the time at which the stored routine or triggering statement began to execute. (Bug #12480)
- `CREATE VIEW` inside a stored procedure caused a server crash if the table underlying the view had been deleted. (Bug #12468)
- Deadlock occurred when several account management statements were run (particularly between `FLUSH PRIVILEGES/SET PASSWORD` and `GRANT/REVOKE` statements). (Bug #12423)
- `InnoDB` was too permissive with `LOCK TABLE ... READ LOCAL` and permitted new inserts into the table. Now `READ LOCAL` is equivalent to `READ` for `InnoDB`. This will cause slightly more locking in `mysqldump`, but makes `InnoDB` table dumps consistent with `MyISAM` table dumps. (Bug #12410)
- If a stored function invoked from a `SELECT` failed with an error, it could cause the client connection to be dropped. Now such errors generate warnings instead so as not to interrupt the `SELECT`. (Bug #12379)
- The value of `character_set_results` could be set to `NULL`, but returned the string `"NULL"` when retrieved. (Bug #12363)
- On Windows, the server was preventing tables from being created if the table name was a prefix of a forbidden name. For example, `nul` is a forbidden name because it is the same as a Windows device name, but a table with the name of `n` or `nu` was being forbidden as well. (Bug #12325)
- `ALTER TABLE ... DISCARD TABLESPACE` for non-`InnoDB` table caused the client to lose the connection. (The server was not returning the error properly.) (Bug #12207)
- Outer join elimination was erroneously applied for some queries that used a `NOT BETWEEN` condition, an `IN(value_list)` condition, or an `IF()` condition. (Bug #12102, Bug #12101)

- Foreign keys were not properly enforced in `TEMPORARY` tables. Foreign keys are no longer permitted in `TEMPORARY` tables. (Bug #12084)
- When using a cursor, a `SELECT` statement that uses a `GROUP BY` clause could return incorrect results. (Bug #11904)
- The `character_set_system` system variable could not be selected with `SELECT @@character_set_system`. (Bug #11775)
- A memory leak resulting from repeated `SELECT ... INTO` statements inside a stored procedure could cause the server to crash. (Bug #11333)
- Use of yaSSL for a secure client connection caused `LOAD DATA LOCAL INFILE` to fail. (Bug #11286)
- `mysqld_multi` now quotes arguments on command lines that it constructs to avoid problems with arguments that contain shell metacharacters. (Bug #11280)
- The server permitted privileges to be granted explicitly for the `INFORMATION_SCHEMA` database. Such privileges are always implicit and should not be grantable. (Bug #10734)
- `SHOW CREATE PROCEDURE` and `SHOW CREATE FUNCTION` no longer qualify the routine name with the database name, for consistency with the behavior of `SHOW CREATE TABLE`. (Bug #10362)
- The server incorrectly generated an `Unknown table` error message when for attempts to drop tables in the `INFORMATION_SCHEMA` database. Now it issues an `Access denied` message. (Bug #9846)
- Within a stored procedure, fetching a large number of rows in a loop using a cursor could result in a server crash or an out of memory error. Also, values inserted within a stored procedure using a cursor were interpreted as `latin1` even if character set variables had been set to a different character set. (Bug #9819, Bug #6513)
- The server permitted `TEMPORARY` tables and stored procedures to be created in the `INFORMATION_SCHEMA` database. (Bug #9683, Bug #10708)
- `SHOW FIELDS` truncated the `TYPE` column to 40 characters. (Bug #7142)

References: See also: Bug #12817.

- A view-creation statement of the form `CREATE VIEW name AS SELECT ... FROM tbl_name AS name` failed with a `Not unique table/alias: 'name'` error. (Bug #6808)
- `myisampack` did not properly pack `BLOB` values larger than 2^{24} bytes. (Bug #4214)

Changes in MySQL 5.0.12 (2005-09-02)

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- **Incompatible Change:** Beginning with MySQL 5.0.12, natural joins and joins with `USING`, including outer join variants, are processed according to the SQL:2003 standard. The changes include elimination of redundant output columns for `NATURAL` joins and joins specified with a `USING` clause and proper ordering of output columns. The precedence of the comma operator also now is lower compared to `JOIN`.

In addition, a `Duplicate column name error` no longer occurs when selecting from a view defined as `SELECT *` from a join that uses a `USING` clause on tables that have a common column name.

These changes make MySQL more compliant with standard SQL. However, they can result in different output columns for some joins. Also, some queries that appeared to work correctly prior to 5.0.12 must be rewritten to comply with the standard. For details about the scope of the changes and examples that show what query rewrites are necessary, see [JOIN Syntax](#). (Bug #6495, Bug #6136, Bug #10972, Bug #9978, Bug #10428, Bug #10646, Bug #6276, Bug #6489, Bug #6558, Bug #9067, Bug #4789, Bug #12065, Bug #13551)

- **MySQL Cluster:** The parsing of the `CLUSTERLOG` command by `ndb_mgm` was corrected to permit multiple items. (Bug #12833)
- **Replication:** Interleaved execution of stored procedures and functions could be written to the binary log incorrectly, causing replication slaves to get out of sync. (Bug #12335)
- **Replication:** Calls to stored procedures were written to the binary log even within transactions that were rolled back, causing them to be executed on replication slaves. (Bug #12334)
- A query of the form `SHOW TABLE STATUS FROM db_name WHERE name IN (select_query)` would crash the server. (Bug #12636)
- Using `DESCRIBE` on a view after renaming a column in one of the view's base tables caused the server to crash. (Bug #12533)
- If a thread (connection) has tables locked, the query cache is switched off for that thread. This prevents invalid results where the locking thread inserts values between a second thread connecting and selecting from the table. (Bug #12385)
- `SHOW TABLE STATUS FROM INFORMATION_SCHEMA` now sorts output by table name the same as it does for other databases. (Bug #12315)
- It is no longer possible to issue `FLUSH` statements from within stored functions or triggers. See [Restrictions on Stored Programs](#), for details. (Bug #12280, Bug #12307)
- `SHOW OPEN TABLES` now supports `FROM` and `LIKE` clauses. (Bug #12183)
- Recursive triggers are detected and not permitted. Also, within a stored function or trigger, it is not permissible to modify a table that is already being used (for reading or writing) by the statement that invoked the function or trigger. (Bug #11896, Bug #12644)
- `INFORMATION_SCHEMA` objects are now reported as a `SYSTEM VIEW` table type. (Bug #11711)
- The stability of cursors when used with `InnoDB` tables was greatly improved. (Bug #11309, Bug #11832, Bug #12243)
- Trying to drop the default keycache by setting `@global.key_buffer_size` to zero now returns a warning that the default keycache cannot be dropped. (Bug #10473)
- `SHOW ENGINE INNODB STATUS` now can display longer query strings. (Bug #7819)
- Added the `SLEEP()` function, which pauses for the number of seconds given by its argument. (Bug #6760)
- `SHOW TABLE STATUS` for a view now shows `VIEW` in uppercase, consistent with `SHOW TABLES` and `INFORMATION_SCHEMA`. (Bug #5501)

Bugs Fixed

- **MySQL Cluster:** When it could not copy a fragment, `ndbd` exited without printing a message about the condition to the error log. Now the message is written. (Bug #12900)

- **MySQL Cluster:** When a `Disk is full` condition occurred, `ndbd` exited without reporting this condition in the error log. (Bug #12716)
- **MySQL Cluster:** Cluster failed to take character set data into account when recomputing hashes (and thus could not locate records for updating or deletion) following a configuration change and node restart. (Bug #12220)
- **MySQL Cluster:** An `ALTER TABLE` statement caused loss of data stored prior to the issuing of the command. (Bug #12118)
- **MySQL Cluster:** Invalid values in `config.ini` caused `ndb_mgmd` to crash. (Bug #12043)
- **MySQL Cluster:** When a schema was detected to be corrupt, `ndb` neglected to close it, resulting in a `file already open` error if the schema was opened again later. (Bug #12027)
- **MySQL Cluster:** Improved error messages related to file system issues. (Bug #11218)
- **MySQL Cluster:** The wrong error message was displayed when the cluster management server port was closed while a `mysqld` process was trying to connect. (Bug #10950)
- **Replication:** Some statements executed on a master server caused the SQL thread on a slave to run out of memory. (Bug #12532)
- **Replication:** Trigger and stored procedure execution could break replication. (Bug #12482)
- **Replication:** `NOW()`, `CURRENT_TIME()` and values generated by timestamp columns are now constant for the duration of a stored function or trigger. This prevents the breaking of statement-based replication. (Bug #12481)
- **Replication:** Slave I/O threads were considered to be in the running state when launched (rather than after successfully connecting to the master server), resulting in incorrect `SHOW SLAVE STATUS` output. (Bug #10780)
- **Replication:** If a `DROP DATABASE` fails on a master server due to the presence of a nondatabase file in the database directory, the master have the database tables deleted, but not the slaves. To deal with failed database drops, we now write `DROP TABLE` statements to the binary log for the tables so that they are dropped on slaves. (Bug #4680)
- An optimizer estimate of zero rows for a nonempty `InnoDB` table used in a left or right join could cause incomplete rollback for the table. (Bug #12779)
- `mysql_fix_privilege_tables.sql` was missing a comma, causing a syntax error when executed. (Bug #12705)
- Invocations of the `SLEEP()` function incorrectly could be optimized away for statements in which it occurs. Statements containing `SLEEP()` incorrectly could be stored in the query cache. (Bug #12689)
- Improper use of loose index scan in `InnoDB` sometimes caused incorrect query results. (Bug #12672)
- A `SELECT DISTINCT` query with a constant value for one of the columns would return only a single row. (Bug #12625)
- `SHOW TABLES FROM` returned the wrong error message if the schema specified did not exist. (Bug #12591)
- A server crash could result from an update of a view defined as a join, even though the update updated only a single table. (Bug #12569)

- `DELETE` or `UPDATE` for an indexed `MyISAM` table could fail. This was due to a change in end-space comparison behavior from 4.0 to 4.1. (Bug #12565)
- The `COLUMN_DEFAULT` column of the `INFORMATION_SCHEMA.COLUMNS` table should be returned as `NULL` if a column has no default value. An empty string was being returned if the column was defined as `NOT NULL`. (Bug #12518)
- The `ROW()` constructor returned an incorrect result when comparison involved `NULL` values. (Bug #12509)
- `STRCMP()` was not handled correctly in views. (Bug #12489)
- Selecting from a view defined as a join over many tables could result in a server crash due to miscalculation of the number of conditions in the `WHERE` clause. (Bug #12470)
- `MEMORY` tables using `B-Tree` index on 64-bit platforms could produce false table is full errors. (Bug #12460)
- The `CREATE_OPTIONS` column of `INFORMATION_SCHEMA.TABLES` showed incorrect options for tables in `INFORMATION_SCHEMA`. (Bug #12397)
- Mishandling of comparison for rows containing `NULL` values against rows produced by an `IN` subquery could cause a server crash. (Bug #12392)
- Selecting from a view after `INSERT` statements for the view's underlying table yielded different results than subsequent selects. (Bug #12382)
- Concatenating `USER()` or `DATABASE()` with a column produced invalid results. (Bug #12351)
- Comparison of `InnoDB` multi-part primary keys that include `VARCHAR` columns can result in incorrect results. (Bug #12340)
- Renamed the `rest()` macro in `my_list.h` to `list_rest()` to avoid name clashes with user code. (Bug #12327)
- When restoring `INFORMATION_SCHEMA` as the default database after failing to execute a stored procedure in an inaccessible database, the server returned a spurious `ERROR 42000: Unknown database 'information_schema'` message. (Bug #12318)
- Users created using an IP address or other alias rather than a host name listed in `/etc/hosts` could not set their own passwords. (Bug #12302)
- The `NUMERIC_SCALE` column of the `INFORMATION_SCHEMA.COLUMNS` table should be returned as `0` for integer columns. It was being returned as `NULL`. (Bug #12301)
- Creating a view that included the `TIMESTAMPDIFF()` function resulted in a invalid view. (Bug #12298)
- The `CHECKSUM TABLE` statement returned incorrect results for tables with deleted rows. After upgrading, users who used stored checksum information to detect table changes should rebuild their checksum data. (Bug #12296)
- Inserting `NULL` into a `GEOMETRY` column for a table that has a trigger could result in a server crash if the table was subsequently dropped. (Bug #12281)
- `mysampack` failed to delete `.TMD` temporary files when run with the `-T` option. (Bug #12235)
- A race condition between server threads could cause a crash if one thread deleted a stored routine while another thread was executing a stored routine. (Bug #12228)

- Duplicate instructions in stored procedures resulted in incorrect execution when the optimizer optimized the duplicate code away. (Bug #12168)
- `XA` permitted two active transactions to be started with the same XID. (Bug #12162)
- `NULL` column definitions were read incorrectly for inner tables of nested outer joins. (Bug #12154)
- `GROUP_CONCAT` ignored the `DISTINCT` modifier when used in a query joining multiple tables where one of the tables had a single row. (Bug #12095)
- A failure to obtain a lock for a `LOCK IN SHARE MODE` query could result in a server crash. (Bug #12082)
- `SELECT ... INTO var_name` within a trigger could cause a server crash. (Bug #11973)
- Using cursors and nested queries for the same table, corrupted results were returned for the outer query. (Bug #11909)
- A query using a `LEFT JOIN`, an `IN` subquery on the outer table, and an `ORDER BY` clause, caused the server to crash when cursors were enabled. (Bug #11901)
- A `UNION` query with `FULLTEXT` could cause server crash. (Bug #11869)
- Some subqueries of the form `SELECT ... WHERE ROW(...) IN (subquery)` were being handled incorrectly. (Bug #11867)
- Column names in subqueries must be unique, but were not being checked for uniqueness. (Bug #11864)
- `TRUNCATE TABLE` did not work with `TEMPORARY InnoDB` tables. (Bug #11816)
- The `mysql_info()` C API function could return incorrect data when executed as part of a multi-statement that included a mix of statements that do and do not return information. (Bug #11688)
- A trigger that included a `SELECT` statement could cause a server crash. (Bug #11587)
- Built-in commands for the `mysql` client, such as `delimiter` and `\d`, are now always parsed within files that are read using the `\.` and `source` commands. (Bug #11523)
- Added portability check for Intel compiler to address a problem compiling `InnoDB` code. (Bug #11510)
- `ALTER TABLE db_name.t RENAME t` did not move the table to default database unless the new name was qualified with the database name. (Bug #11493)
- Joins on `VARCHAR` columns of different lengths could produce incorrect results. (Bug #11398)
- For PKG installs on Mac OS X, the preinstallation and postinstallation scripts were being run only for new installations and not for upgrade installations, resulting in an incomplete installation process. (Bug #11380)
- Prepared statement parameters could cause errors in the binary log if the character set was `cp932`. (Bug #11338)
- Columns defined as `TINYINT(1)` were redefined as `TINYINT(4)` when incorporated into a `VIEW`. (Bug #11335)
- Stored procedures with particularly long loops could crash the server due to a memory leak. (Bug #11247, Bug #12297)
- `SET GLOBAL TRANSACTION ISOLATION LEVEL` was not working. (Bug #11207)

- It was permitted for a view to depend on a function that referred to a temporary table. (Bug #10970)
- Issuing `FLUSH INSTANCES` followed by `STOP INSTANCE` caused instance manager to crash. (Bug #10957)
- User variables were not automatically cast for comparisons, causing queries to fail if the column and connection character sets differed. Now when mixing strings with different character sets but the same coercibility, permit conversion if one character set is a superset of the other. (Bug #10892)
- An incorrect conversion from `double` to `ulonglong` caused indexes not to be used for `BDB` tables on HP-UX. (Bug #10802)
- `DATE_ADD()` and `DATE_SUB()` were converting invalid dates to `NULL` in `TRADITIONAL` SQL mode rather than rejecting them with an error. (Bug #10627)
- Views with multiple `UNION` and `UNION ALL` produced incorrect results. (Bug #10624)
- It was not possible to create a stored function with a spatial return value data type. (Bug #10499)
- `INSERT ... SELECT ... ON DUPLICATE KEY UPDATE` could fail with an erroneous "Column '`col_name`' specified twice" error. (Bug #10109)
- The only valid values for the `PACK_KEYS` table option are 0 and 1, but other values were being accepted. (Bug #10056)
- Using a stored procedure that referenced tables in the `INFORMATION_SCHEMA` database would return an empty result set. (Bug #10055, Bug #12278)
- `FLUSH TABLES WITH READ LOCK` combined with `LOCK TABLE .. WRITE` caused deadlock. (Bug #9459)
- A data type of `CHAR BINARY` was not recognized as valid for stored routine parameters. (Bug #9048)
- `ISO-8601` formatted dates were not being parsed correctly. (Bug #7308)
- On Windows when the `--innodb_buffer_pool_ave_mem_mb` option has been given, the server detects whether AWE support is available and has been compiled into the server, and displays an appropriate error message if not. (Bug #6581)
- Pathname values for options such as `--basedir` or `--datadir` didn't work on Japanese Windows machines for directory names containing multibyte characters having a second byte of `0x5C` ("\`\`"). (Bug #5439)
- `SHOW TABLE STATUS` sometimes reported a `Row_format` value of `Dynamic` for `MEMORY` tables, though such tables always have a format of `Fixed`. (Bug #3094)

Changes in MySQL 5.0.11 (2005-08-06)

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- **MySQL Cluster:** Improved handling of the configuration variables `NoOfPagesToDiskDuringRestartACC`, `NoOfPagesToDiskAfterRestartACC`, `NoOfPagesToDiskDuringRestartTUP`, and `NoOfPagesToDiskAfterRestartTUP` should result in noticeably faster startup times for MySQL Cluster. (Bug #12149)

- Added an optimization that avoids key access with `NULL` keys for the `ref` method when used in outer joins. (Bug #12144)
- Added support of where clause for queries with `FROM DUAL`. (Bug #11745)
- Maximum size of stored procedures increased from 64k to 4Gb. (Bug #11602)
- `SHOW CHARACTER SET` and `INFORMATION_SCHEMA` now properly report the `Latin1` character set as `cp1252`. (Bug #11216)
- Added new `ER_STACK_OVERRUN_NEED_MORE` error message to indicate that, while the stack is not completely full, more stack space is required. (Bug #11213)
- `mysqldump` now dumps triggers for each dumped table. This can be suppressed with the `--skip-triggers` option. (Bug #10431)
- Added error message for users who attempt `CREATE TABLE ... LIKE` and specify a nontable in the `LIKE` clause. (Bug #6859)
- Security improvement: Applied a patch that addresses a potential `zlib` data vulnerability that could result in an application crash. This only affects the binaries for platforms that are linked statically against the bundled `zlib` (most notably Microsoft Windows and HP-UX). (CVE-2005-1849)

Bugs Fixed

- **MySQL Cluster:** The MySQL Cluster backup log was invalid where the number of Cluster nodes was not equal to a power of 2. (Bug #11675)
- Creation of the `mysql` group account failed during the RPM installation. (Bug #12348)
- Updated dependency list for RPM builds to include missing dependencies such as `useradd` and `groupadd`. (Bug #12233)
- A delayed insert that would duplicate an existing record crashed the server instead. (Bug #12226)
- When `DROP DATABASE` was called concurrently with a `DROP TABLE` of any table, the MySQL Server crashed. (Bug #12212)
- **InnoDB:** True `VARCHAR`: Return `NULL` columns in the format expected by MySQL. (Bug #12186)
- Information about a trigger was not displayed in the output of `SELECT ... FROM INFORMATION_SCHEMA.TRIGGERS` when the selected database was `INFORMATION_SCHEMA`, prior to the trigger's first invocation. (Bug #12127)
- **InnoDB:** Do not flush after each write, not even before setting up the doublewrite buffer. Flushing can be extremely slow on some systems. (Bug #12125)
- Two threads could potentially initialize different characters sets and overwrite each other. (Bug #12109)
- `big5` strings were not being stored in `FULLTEXT` index. (Bug #12075)
- Character data truncated when GBK characters `0xA3A0` and `0xA1` are present. (Bug #11987)
- `ALTER TABLE` when `sql_mode = 'TRADITIONAL'` gave rise to an invalid error message. (Bug #11964)
- Issuing successive `FLUSH TABLES WITH READ LOCK` would cause the `mysql` client to hang. (Bug #11934)

- `mysql_install_db` used static `localhost` value in `GRANT` tables even when server host name is not `localhost`, such as `localhost.localdomain`. This change is applied to version 5.0.10b on Windows. (Bug #11822)
- Comparisons like `SELECT "A\\" LIKE "A\\";` fail when using `SET NAMES utf8;` (Bug #11754)
- Attempting to repair a table having a full-text index on a column containing words whose length exceeded 21 characters and where `myisam_repair_threads` was greater than 1 would crash the server. (Bug #11684)
- When used in a `SELECT` query against a view, the `GROUP_CONCAT()` function returned only a single row. (Bug #11412)
- Multiplying `ABS()` output by a negative number would return incorrect results. (Bug #11402)
- The `LPAD()` and `RPAD()` functions returned the wrong length to `mysql_fetch_fields()`. (Bug #11311)
- A `UNIQUE VARCHAR` column would be mis-identified as `MUL` in table descriptions. (Bug #11227)
- DDL statements are now permitted in stored procedures if the procedure is not invoked from a stored function or a trigger. This fix also resolves a problem where a `TEMPORARY` statement created by one stored routine was inaccessible to another routine invoked during the same connection. (Bug #11126)
- Calling the C API function `mysql_stmt_fetch()` after all rows of a result set were exhausted would return an error instead of `MYSQL_NO_DATA`. (Bug #11037)
- `SELECT @@local...` returned `@@session...` in the column header. (Bug #10724)
- Incorrect error message displayed if user attempted to create a table in a nonexisting database using `CREATE database_name.table_name` syntax. (Bug #10407)
- Unsigned `LONG` system variables may return incorrect value when retrieved with a `SELECT` for certain values. (Bug #10351)
- `GROUP_CONCAT()` sometimes returned a result with a different collation from that of its arguments. (Bug #10201)
- Prepared statements were not being written to the Slow Query log. (Bug #9968)
- The value of `max_connections_per_hour` was capped by the unrelated `max_user_connections` setting. (Bug #9947)
- In stored procedures, a cursor that fetched an empty string into a variable would set the variable to `NULL` instead. (Bug #8692)
- Added checks to prevent error when allocating memory when there was insufficient memory available. (Bug #7003)
- Multiple `SELECT SQL_CACHE` queries in a stored procedure causes error and client hang. (Bug #6897)
- A trigger dependent on a feature of one `sql_mode` setting would cause an error when invoked after the `sql_mode` was changed. (Bug #5891)

Changes in MySQL 5.0.10 (2005-07-27)

- [Functionality Added or Changed](#)

- [Bugs Fixed](#)

Functionality Added or Changed

- **Incompatible Change:** The namespace for triggers has changed. Previously, trigger names had to be unique per table. Now they must be unique within the schema (database). An implication of this change is that `DROP TRIGGER` syntax now uses a schema name instead of a table name (schema name is optional and, if omitted, the current schema will be used).



Note

When upgrading from a version of MySQL 5 older than 5.0.10 to MySQL 5.0.10 or newer, you must drop all triggers and re-create them or `DROP TRIGGER` will not work after the upgrade. A suggested procedure for doing this is given in [Changes Affecting Upgrades to 5.0](#).

(Bug #5892)

- **MySQL Cluster:** A new `-P` option is available for use with the `ndb_mgmd` client. When called with this option, `ndb_mgmd` prints all configuration data to `stdout`, then exits.
- On Windows, the search path used by MySQL applications for `my.ini` now includes `..\my.ini` (that is, the application's parent directory, and hence, the installation directory). (Bug #10419)
- The viewing of triggers and trigger metadata has been enhanced as follows:
 - An extension to the `SHOW` command has been added: `SHOW TRIGGERS` can be used to view a listing of triggers. See [SHOW TRIGGERS Syntax](#), for details.
 - The `INFORMATION_SCHEMA` database now includes a `TRIGGERS` table. See [The INFORMATION_SCHEMA TRIGGERS Table](#), for details.

(Bug #9586)

- It is no longer necessary to issue an explicit `LOCK TABLES` for any tables accessed by a trigger prior to executing any statements that might invoke the trigger.

Previously, executing a statement that invoked a trigger would cause problems unless a `LOCK TABLES` was first issued for any tables accessed by the trigger. The exact nature of the problem depended upon the MySQL 5.0 release being used: prior to 5.0.3, this resulted in a crash; from 5.0.3 to 5.0.7, MySQL would issue a warning; in 5.0.9, the server would issue an error.

The same issue caused `LOCK TABLES` to fail following `UNLOCK TABLES` if triggers were involved. (Bug #8406, Bug #9581)

- The MySQL server now starts correctly with all combinations of `--basedir` and `--datadir`, resolving an issue introduced by the original fix for this bug in MySQL 4.1.9. (Bug #7249)

References: See also: Bug #7518.

- Added `mysql_get_character_set_info()` C API function for obtaining information about the default character set of the current connection.
- An extension to the `SHOW` statement has been added: `SHOW TRIGGERS` can be used to view a listing of triggers. See [SHOW TRIGGERS Syntax](#), for details.
- Add the `--defaults-group-suffix` option. See [Using Option Files](#).

- The bundled version of the `readline` library was upgraded to version 5.0.
- Triggers can now reference tables by name. See [CREATE TRIGGER Syntax](#), for more information.
- Add `table_lock_wait_timeout` global system variable.

Bugs Fixed

- **Security Fix:** A vulnerability in `zlib` could result in a buffer overflow and arbitrary code execution. (Bug #11844, CVE-2005-2096, CVE-2005-1849)
- **MySQL Cluster:** The temporary tables created by an `ALTER TABLE` on an `NDB` table were visible to all SQL nodes in the cluster. (Bug #12055)
- **MySQL Cluster:** `NDB` ignored the `Hostname` option in the `[ndbd default]` section of the cluster configuration file. (Bug #12028)
- **MySQL Cluster:** The output of `percona --help` did not display any information about the `--ndb` option. (Bug #11999)
- **MySQL Cluster:** Attempting to create or drop tables during a backup would cause the cluster to shut down. (Bug #11942)
- **MySQL Cluster:** `ndb_mgmd` leaked file descriptors. (Bug #11898)
- **MySQL Cluster:** The MySQL Server left core files following shutdown if data nodes had failed. (Bug #11516)
- **MySQL Cluster:** When attempting to drop a table with a broken unique index, `NDB` failed to drop the table and erroneously report that the table was unknown. (Bug #11355)
- **MySQL Cluster:** Trying to use a greater number of tables than specified by the value of `MaxNoOfTables` caused table corruption such that data nodes could not be restarted. (Bug #9994)
- The server did not compile correctly when using `gcc4` on AMD64 platforms. (Bug #12040)
- `SHOW BINARY LOGS` displayed a file size of 0 for all log files but the current one if the files were not located in the data directory. (Bug #12004)
- Increased the version number of the `libmysqlclient` shared library from 14 to 15 because it is binary incompatible with the MySQL 4.1 client library. (Bug #11893)
- The server crashed when dropping a trigger that invoked a stored procedure, if the procedure was not yet in the connection-specific stored routine cache. (Bug #11889)
- `SELECT ... NOT IN()` gave unexpected results when only static value present between the `()`. (Bug #11885)
- A recent optimizer change caused `DELETE ... WHERE ... NOT LIKE` and `DELETE ... WHERE ... NOT BETWEEN` to not properly identify the rows to be deleted. (Bug #11853)
- Execution of a prepared statement that invoked a nonexistent or dropped stored routine would crash the server. (Bug #11834)
- Selecting the result of an aggregate function for an `ENUM` or `SET` column within a subquery could result in a server crash. (Bug #11821)
- Creating a table with a `SET` or `ENUM` column with the `DEFAULT 0` clause caused a server crash if the table's character set was `utf8`. (Bug #11819)

- Incorrect column values could be retrieved from views defined using statements of the form `SELECT * FROM tbl_name`. (Bug #11771)
- When invoked within a view, `SUBTIME()` returned incorrect values. (Bug #11760)
- For several character sets, MySQL incorrectly converted the character code for the division sign to the `ucjpm` character set. (Bug #11717)
- Performing an `ORDER BY` on a `SELECT` from a `VIEW` produced unexpected results when `VIEW` and underlying table had the same column name on different columns. (Bug #11709)
- Execution of `SHOW TABLES` failed to increment the `Com_show_tables` status variable. (Bug #11685)
- `LIKE` pattern matching using prefix index didn't return correct result. (Bug #11650)
- Invoking the `DES_ENCRYPT()` function could cause a server crash if the server was started without the `--des-key-file` option. (Bug #11643)
- IP addresses not shown in `ndb_mgm SHOW` command on second `ndb_mgmd` (or on `ndb_mgmd` restart). (Bug #11596)
- `SHOW PROCEDURE/FUNCTION STATUS` didn't work for users with limited access. (Bug #11577)
- `mysqlbinlog` was failing the test suite on Windows due to `BOOL` being incorrectly cast to `INT`. (Bug #11567)
- The server crashed upon execution of a statement that used a stored function indirectly (via a view) if the function was not yet in the connection-specific stored routine cache and the statement would update a `Handler_xxx` status variable. This fix enables the use of stored routines under `LOCK TABLES` without explicitly locking the `mysql.proc` table. However, you cannot use `mysql.proc` in statements that will combine locking of it with modifications for other tables. (Bug #11554)
- Aliasing the column names in a `VIEW` did not work when executing a `SELECT` query on the `VIEW`. (Bug #11399)
- The `mysql.proc` table was not being created properly with the proper `utf8` character set and collation, causing server crashes for stored procedure operations if the server was using a multibyte character set. To take advantage of the bug fix, `mysql_fix_privilege_tables` should be run to correct the structure of the `mysql.proc` table.

Note that it is *necessary* to run `mysql_fix_privileges_tables` when upgrading from a previous installation that contains the `mysql.proc` table (that is, from a previous 5.0 installation). Otherwise, creating stored procedures might not work. (Bug #11365)
- For prepared statements, the SQL parser did not disallow “?” parameter markers immediately adjacent to other tokens, which could result in malformed statements in the binary log. (For example, `SELECT * FROM t WHERE? = 1` could become `SELECT * FROM t WHERE0 = 1`.) (Bug #11299)
- The C API function `mysql_stmt_reset()` did not clear error information. (Bug #11183)
- `INFORMATION_SCHEMA.COLUMNS` had some inaccurate values for some data types. (Bug #11057)
- MySQL server would crash is a fetch was performed after a `ROLLBACK` when cursors were involved. (Bug #10760)
- When two threads competed for the same table, a deadlock could occur if one thread also had a lock on another table through `LOCK TABLES` and the thread was attempting to remove the table in some manner while the other thread tried to place locks on both tables. (Bug #10600)

- When used within a subquery, `SUBSTRING()` returned an empty string. (Bug #10269)
- Multiple-table `UPDATE` queries using `CONVERT_TZ()` failed with an error. (Bug #9979)
- With strict SQL mode enabled, `ALTER TABLE` reported spurious “Invalid default value” messages for columns that had no `DEFAULT` clause. (Bug #9881)
- `mysql_fetch_fields()` returned incorrect length information for `MEDIUM` and `LONG TEXT` and `BLOB` columns. (Bug #9735)
- Within a stored procedure, selecting from a table through a view caused subsequent updates to the table to fail with a message that the table was read-locked. (Bug #9597)
- Within a stored procedure that selects from a table, invoking another procedure that requires a write lock for the table caused that procedure to fail with a message that the table was read-locked. (Bug #9565)
- Server-side prepared statements failed for columns with a character set of `ucs2`. (Bug #9442)
- In SQL prepared statements, comparisons could fail for values not equally space-padded. For example, `SELECT 'a' = 'a ';` returns 1, but `PREPARE s FROM 'SELECT ?=?'; SET @a = 'a', @b = 'a '; PREPARE s FROM 'SELECT ?=?'; EXECUTE s USING @a, @b;` incorrectly returned 0. (Bug #9379)
- References to system variables in an SQL statement prepared with `PREPARE` were evaluated during `EXECUTE` to their values at prepare time, not to their values at execution time. (Bug #9359)
- The server did not accept some fully qualified trigger names. (Bug #8758)
- Creating a trigger in one database that references a table in another database was being permitted without generating errors. (Bug #8751)
- For a stored procedure defined with `SQL SECURITY DEFINER` characteristic, `CURRENT_USER()` incorrectly reported the user invoking the procedure, not the user who defined it. (Bug #7291)
- Labels in stored routines did not work if the character set was not `latin1`. (Bug #7088)
- Duplicate trigger names were permitted within a single schema. (Bug #6182)
- For execution of a stored procedure that refers to a view, changes to the view definition were not seen. The procedure continued to see the old contents of the view. (Bug #6120)
- The `traditional` SQL mode accepted invalid dates if the date value provided was the result of an implicit type conversion. (Bug #5906)
- In a shared Windows environment, MySQL could not find its configuration file unless the file was in the `C:\` directory. (Bug #5354)
- Functions that evaluate to constants (such as `NOW()` and `CURRENT_USER()`) were being evaluated in the definition of a `VIEW` rather than included verbatim. (Bug #4663)

Changes in MySQL 5.0.9 (2005-07-15)

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- The handling of `BIT` columns has been improved, and should now be much more reliable in a number of cases. (Bug #11572, Bug #11091, Bug #10617)
- Recursion in stored routines is now disabled because it was crashing the server. (Bug #11394)
- An attempt to create a `TIMESTAMP` column with a display width (for example, `TIMESTAMP(6)`) now results in a warning. Display widths have not been supported for `TIMESTAMP` since MySQL 4.1. (Bug #10466)
- `mysql_real_escape_string()` API function now respects `NO_BACKSLASH_ESCAPES` SQL mode. (Bug #10214)
- `InnoDB`: Made `CHECK TABLE` killable. (Bug #9730)
- `InnoDB`: Make `innodb_thread_concurrency = 20` by default. Bypass the concurrency checking if the setting is greater than or equal to 20.
- `InnoDB`: Various optimizations. Removed unreachable debug code from nondebug builds. Added hints for the branch predictor in `gcc`. Made assertions occupy less space.
- `InnoDB`: When creating or extending an `InnoDB` data file, at most one megabyte at a time is allocated for initializing the file. Previously, `InnoDB` allocated and initialized 1 or 8 megabytes of memory, even if only a few 16-kilobyte pages were to be written. This improves the performance of `CREATE TABLE` in `innodb_file_per_table` mode.

Bugs Fixed

- **MySQL Cluster**: When trying to open a table that could not be discovered or unpacked, the cluster returned error codes which the MySQL server falsely interpreted as operating system errors. (Bug #10365)
- The `--master-data` option for `mysqldump` resulted in no error if the binary log was not enabled. Now an error occurs unless the `--force` option is given. (Bug #11678)
- When a table had a primary key containing a `BLOB` column, creation of another index failed with the error `BLOB/TEXT column used in key specification without keylength`, even when the new index did not contain a `BLOB` column. (Bug #11657)
- Incorrect results when using `GROUP BY ... WITH ROLLUP` on a `VIEW`. (Bug #11639)
- MySQL would not compile correctly on QNX due to missing `rint()` function. (Bug #11544)
- A `SELECT DISTINCT col_name` would work correctly with a `MyISAM` table only when there was an index on `col_name`. (Bug #11484)
- Using `CONCAT_WS()` on a column set `NOT NULL` caused incorrect results when used in a `LEFT JOIN`. (Bug #11469)
- Temporary tables were created in the data directory instead of `tmpdir`. (Bug #11440)
- Running a `CHECK TABLES` on multiple views crashed the server. (Bug #11337)
- Manually inserting a row with `host= ''` into `mysql.tables_priv` and performing a `FLUSH PRIVILEGES` would cause the server to crash. (Bug #11330)
- Wrong comparison method used in `VIEW` when relaxed date syntax used (for example, `2005.06.10`). (Bug #11325)
- Signed `BIGINT` would not accept `-9223372036854775808` as a `DEFAULT` value. (Bug #11215)

- Optimizer performed range check when comparing unsigned integers to negative constants, could cause errors. (Bug #11185)
- A cursor using a query with a filter on a `DATE` or `DATETIME` column would cause the server to crash server after the data was fetched. (Bug #11172)
- The `mysql_config` script did not handle symbolic linking properly. (Bug #10986)
- `mysqldump` failed when reloading a view if the view was defined in terms of a different view that had not yet been reloaded. `mysqldump` now creates a dummy table to handle this case. (Bug #10927)
- If a prepared statement cursor is opened but not completely fetched, attempting to open a cursor for a second prepared statement will fail. (Bug #10794)
- Combining cursors and subqueries could cause server crash or memory leaks. (Bug #10736)
- Instances of the `VAR_SAMP()` function in view definitions were converted to `VARIANCE()`. This is incorrect because `VARIANCE()` is the same as `VAR_POP()`, not `VAR_SAMP()`. (Bug #10651)
- `DES_ENCRYPT()` and `DES_DECRYPT()` require SSL support to be enabled, but were not checking for it. Checking for incorrect arguments or resource exhaustion was also improved for these functions. (Bug #10589)
- For `MEMORY` tables, it was possible for updates to be performed using outdated key statistics when the updates involved only very small changes in a very few rows. This resulted in the random failures of queries such as `UPDATE t SET col = col + 1 WHERE col_key = 2;` where the same query with no `WHERE` clause would succeed. (Bug #10178)
- When used in joins, `SUBSTRING()` failed to truncate to zero those string values that could not be converted to numbers. (Bug #10124)
- Views did not use indexes on all appropriate queries. (Bug #10031)
- Closing a cursor that was already closed would cause MySQL to hang. (Bug #9814)
- The server would lose table-level `CREATE VIEW` and `SHOW VIEW` privileges following a `FLUSH PRIVILEGES` or server restart. (Bug #9795)
- `mysqldump --xml` did not format `NULL` column values correctly. (Bug #9657)
- The `--no-data` option for `mysqldump` was being ignored if table names were given after the database name. (Bug #9558)
- Clients would hang following some errors with stored procedures. (Bug #9503)
- `mysqldump` could crash for illegal or nonexistent table names. (Bug #9358)
- A compression algorithm issue caused `myisampack` to fail for very large data sets (where the total size of all records in a single column was on the order of 3 GB or more) on 64-bit platforms. (A fix for other platforms was made in MySQL 5.0.6.) (Bug #8321)
- The `ENCRYPT()` and `SUBSTRING_INDEX()` functions would cause errors when used with a `VIEW`. (Bug #7024)
- `SHOW CREATE VIEW` did not take the `ANSI SQL` mode into account when quoting identifiers. (Bug #6903)
- In strict mode, an `INSERT` into a view that did not include a value for a `NOT NULL` column but that did include a `WHERE` test on the same column would succeed, This happened even though the `INSERT` should have been prevented due to the failure to supply a value for the `NOT NULL` column. (Bug #6443)

Changes in MySQL 5.0.8 (Not released)



Note

Starting with version 5.0.8, changes for MySQL Cluster can be found in the combined Change History.

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- **Incompatible Change:** Previously, conversion of `DATETIME` values to numeric form by adding zero produced a result in `YYYYMMDDHHMMSS` format. The result of `DATETIME+0` is now in `YYYYMMDDHHMMSS.000000` format. (Bug #12268)
- **Replication:** Some data definition statements (`CREATE TABLE` where the table was not a temporary table, `TRUNCATE TABLE`, `DROP DATABASE`, and `CREATE DATABASE`) were not being written to the binary log after a `ROLLBACK`. This also caused problems with replication.



Important

As a result of this fix, the following statements now cause an implicit commit:

- `CREATE TABLE`
- `TRUNCATE TABLE`
- `DROP DATABASE`
- `CREATE DATABASE`

(Bug #6883)

- Where a `GROUP BY` query uses a grouping column from the query's `SELECT` clause, MySQL now issues a warning. This is done because the SQL standard states that any grouping column must unambiguously reference a column of the table resulting from the query's `FROM` clause, and permitting columns from the `SELECT` clause to be used as grouping columns is a MySQL extension to the standard.

By way of example, consider the following table:

```
CREATE TABLE users (
  userid INT NOT NULL PRIMARY KEY,
  username VARCHAR(25),
  usergroupid INT NOT NULL
);
```

MySQL enables you to use the alias in this query:

```
SELECT usergroupid AS id, COUNT(userid) AS number_of_users
FROM users
GROUP BY id;
```

However, the SQL standard requires that the column name be used, as shown here:

```
SELECT usergroupid AS id, COUNT(userid) AS number_of_users
```

```
FROM users
GROUP BY usergroupid;
```

Queries such as the first of the two shown above will continue to be supported in MySQL; however, beginning with MySQL 5.0.8, using a column alias in this fashion will generate a warning. Note that in the event of a collision between column names or aliases used in joins, MySQL attempts to resolve the conflict by giving preference to columns arising from tables named in the query's `FROM` clause. (Bug #11211)

- Using prepared statements within a stored routine (`PREPARE`, `EXECUTE`, `DEALLOCATE PREPARE`) could cause the client connection to be dropped after the routine returned. In addition, executing a statement which called a function deallocating the same statement caused the server to crash. This is prevented by disabling dynamic SQL within stored routines.



Note

This restriction was lifted in 5.0.13 for stored procedures, but not stored functions or triggers.

(Bug #10975, Bug #10605)

References: See also: Bug #7115.

- Added support for `B'10'` syntax for bit literal. (Bug #10650)
- `MEMORY` tables now support indexes of up to 500 bytes. See [The MEMORY \(HEAP\) Storage Engine](#). (Bug #10566)
- Expanded on information provided in general log and slow query log for prepared statements. (Bug #8367, Bug #9334)
- New `sql_mode` mode `NO_ENGINE_SUBSTITUTION` prevents automatic substitution of storage engine when the requested storage engine is disabled or not compiled in. (Bug #6877)

Bugs Fixed

- Security Fix:** On Windows systems, a user with any of the following privileges on `*.*` could crash `mysqld` by issuing a `USE LPT1;` or `USE PRN;` command:
 - `REFERENCES`
 - `CREATE TEMPORARY TABLES`
 - `GRANT OPTION`
 - `CREATE`
 - `SELECT`

In addition, any of the commands `USE NUL;`, `USE CON;`, `USE COM1;`, or `USE AUX;` would report success even though the database was not in fact changed.



Note

Although this bug was thought to be fixed previously, it was later discovered to be present in the MySQL 5.0.7-beta release for Windows.

(Bug #9148)

- **MySQL Cluster:** Setting `TransactionInactiveTimeout = 0` did not result in an infinite timeout. (Bug #11290)
- **MySQL Cluster:** `mysqld` processes did not reconnect to the cluster following a restart of `ndb_mgmd`. (Bug #11221)
- **MySQL Cluster:** Insert records were incorrectly applied by `ndb_restore`, thus making restoring from backup inconsistent if the binary log contained inserts. (Bug #11166)
- **MySQL Cluster:** A `DELETE` performed as part of a transaction caused an erroneous result. (Bug #11133)
- **MySQL Cluster:** Connections between data nodes and management nodes were not closed following shutdown of `ndb_mgmd`. (Bug #11132)
- **MySQL Cluster:** The `ndb_mgm` client's `SHOW` command displayed incorrect output after master data node failure. (Bug #11050)
- **MySQL Cluster:** When using dynamically allocated ports on Linux, the cluster would hang on initial startup. (Bug #10893)
- **MySQL Cluster:** Not permitting sufficient parallelism in the cluster's configuration (for example, by setting `NoOfTransactions` too small) caused `ndb_restore` to fail without providing any error messages. (Bug #10294)
- **MySQL Cluster:** Running `ndb_select_count` crashed the cluster when running on Red Hat Enterprise 4/64-bit/Opteron. (Bug #10058)
- **MySQL Cluster:** Data nodes failed to restart on 64-bit Solaris. (Bug #9025)
- **MySQL Cluster:** On 64-bit Solaris 9, the cluster timed out and crashed after the first query was made. (Bug #8918)
- **Replication:** An invalid comparison caused warnings for packet length in replication on 64-bit compilers. (Bug #11064)
- Multiple range accesses in a subquery cause server crash. (Bug #11487)
- A `CAST()` value could not be included in a `VIEW`. (Bug #11387)
- Server crashed when using `GROUP BY` on the result of a `DIV` operation on a `DATETIME` value. (Bug #11385)
- `INSERT INTO SELECT FROM view` produced incorrect result when using `ORDER BY`. (Bug #11298)
- Possible `NULL` values in `BLOB` columns could crash the server when a `BLOB` was used in a `GROUP BY` query. (Bug #11295)
- An outer join with an `ON` condition that evaluated to false could return an incorrect result. (Bug #11285)
- An outer join with an empty derived table (a result from a subquery) returned no result. (Bug #11284)
- `CAST(... AS DECIMAL)` didn't work for strings. (Bug #11283)
- Corrected a problem with `IFNULL()` returning an incorrect result on 64-bit systems. (Bug #11235)
- The `SHOW INSTANCE OPTIONS` command in MySQL Instance Manager displayed option values incorrectly for options for which no value had been given. (Bug #11200)
- The default host name for MySQL server was always `mysql`. (Bug #11174)

- Some internal functions did not take into account that, for multibyte character sets, `CHAR` columns could exceed 255 bytes and `VARCHAR` columns could exceed 65,535 bytes, which could cause the server to crash. (Bug #11167)
- There were locking problems with multiple-statement `DELETE` statements performed within a stored routine, such as incorrectly locking the table to be read with a read lock rather than a write lock. (Bug #11158)
- Testing for `crypt()` support caused compilation problems when using OpenSSL/yaSSL on HP-UX and Mac OS X. (Bug #11150, Bug #10675)
- The `NULLIF()` function could produce incorrect results if the first argument was `NULL`. (Bug #11142)
- `mysqld_safe` would sometimes fail to remove the pid file for the old `mysql` process after a crash. As a result, the server failed to start due to a false `A mysqld process already exists...` error. (Bug #11122)
- Calling a stored procedure that made use of an `INSERT ... SELECT ... UNION SELECT ...` query caused a server crash. (Bug #11060)
- `sql_data_access` column of `routines` table of `INFORMATION_SCHEMA` was empty. (Bug #11055)
- `SELECT DISTINCT` queries or `GROUP BY` queries without `MIN()` or `MAX()` could return inconsistent results for indexed columns. (Bug #11044)
- A `CREATE TABLE db_name.tbl_name LIKE ...` statement would crash the server when no database was selected. (Bug #11028)
- On Windows, `mysqlshow` did not interpret wildcard characters properly if they were given in the table name argument. (Bug #10947)
- The host name cache was not working. (Bug #10931)
- A three byte buffer overflow in the client functions caused improper exiting of the client when reading a command from the user. (Bug #10841)
- The `mysql` client would output a prompt twice following input of very long strings, because it incorrectly assumed that a call to the `_cgets()` function would clear the input buffer. (Bug #10840)
- Setting `@@sql_mode = NULL` caused an erroneous error message. (Bug #10732)
- When using a cursor with a prepared statement, the first execution returned the correct result but was not cleaned up properly, causing subsequent executions to return incorrect results. (Bug #10729)
- Converting a `VARCHAR` column having an index to a different type (such as `TINYTEXT`) gave rise to an incorrect error message.

Note that this bug fix induces a slight change in the behavior of indexes: If an index is defined to be the same length as a field (or is left to default to that field's length), and the length of the field is later changed, then the index will adopt the new length of the field. Previously, the size of the index did not change for some field types (such as `VARCHAR`) when the field type was changed. (Bug #10543)

- `InnoDB`: Pad UTF-8 `VARCHAR` columns with `0x20`. Pad UCS2 `CHAR` columns with `0x0020`. (Bug #10511)
- `InnoDB`: Enforce maximum `CHAR_LENGTH()` of UTF-8 data in `ON UPDATE CASCADE`. (Bug #10409)
- `SELECT * FROM table` returned incorrect results when called from a stored procedure, where `table` had a primary key. (Bug #10136)

- The granting and revocation of privileges on a stored routine was performed when running the server with `--skip-grant-tables` even after the statement `SET @@GLOBAL.automatic_sp_privileges = 1;` was executed. (Bug #9993)
- A stored procedure run while the query cache was enabled could cause the server to crash. (Bug #9715)
- Table names were not handled correctly when `lower_case_table_names = 2` if the table name lettercase differed in the `FROM` and `WHERE` clauses. (Bug #9500)
- `SHOW CREATE DATABASE INFORMATION_SCHEMA` returned an “unknown database” error. (Bug #9434)
- `SELECT DISTINCT ... GROUP BY constant` returned multiple rows (it should return a single row). (Bug #8614)
- An issue with index merging could cause suboptimal index merge plans to be chosen when searching by indexes created on `DATE` columns. The same issue caused the `InnoDB` storage engine to issue the warning `using a partial-field key prefix in search`. (Bug #8441)
- The `mysqlhotcopy` script was not parsing the output of `SHOW SLAVE STATUS` correctly when called with the `--record_log_pos` option. (Bug #7967)
- A Boolean full-text search where a query contained more query terms than one-third of the query length caused the server to hang or crash. (Bug #7858)
- When used in defining a view, the `TIME_FORMAT()` function failed with calculated values, for example, when passed the value returned by `SEC_TO_TIME()`. (Bug #7521)
- Views could be created with duplicate column names. (Bug #7448)
- An `ORDER BY` clause sometimes had no effect on the ordering of a result when selecting specific columns (as opposed to using `SELECT *`) from a view. (Bug #7422)
- Using `PREPARE` to prepare a statement that invoked a stored routine that executed the prepared statement caused a `Packets out of order error` the second time the routine was invoked. This is prevented by disabling dynamic SQL within stored routines.



Note

This restriction was lifted in 5.0.13 for stored procedures, but not for stored functions or triggers.

(Bug #7115)

References: See also: Bug #10975, Bug #10605.

- Selecting from a view defined using `SELECT SUM(DISTINCT ...)` caused an error; attempting to execute a `SELECT * FROM INFORMATION_SCHEMA.TABLES` query after defining such a view crashed the server. (Bug #7015)

Changes in MySQL 5.0.7 (2005-06-10)

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- **Security Fix:** A UDF library-loading vulnerability could result in a buffer overflow and code execution. (CVE-2005-2558)
- Improved the optimizer to be able to use indexes for expressions of the form `indexed_col NOT IN (val1, val2, ...)` and `indexed_col NOT BETWEEN val1 AND val2`. (Bug #10561)
- The `table`, `type`, and `rows` columns of `EXPLAIN` output can now be `NULL`. This is required for using `EXPLAIN` on `SELECT` queries that use no tables, such as `EXPLAIN SELECT 1`. (Bug #9899)
- All characters occurring on the same line following the `DELIMITER` keyword will be set as delimiter. For example, `DELIMITER ;` will set `;` as the delimiter. This behavior is now consistent between MySQL 5.1 and MySQL 5.0. (Bug #9879)
- Added `mysql_set_character_set()` C API function for setting the default character set of the current connection. This enables clients to affect the character set used by `mysql_real_escape_string()`. (Bug #8317)
- The `--delayed-insert` option for `mysqldump` was disabled to avoid causing problems with storage engines that do not support `INSERT DELAYED`. (Bug #7815)
- Placeholders now can be used for `LIMIT` in prepared statements. (Bug #7306)
- **InnoDB:** In stored procedures and functions, **InnoDB** no longer takes full explicit table locks for every involved table. Only “intention” locks are taken, similar to those in the execution of an ordinary SQL statement. This greatly reduces the number of deadlocks.
- `SHOW BINARY LOGS` now displays a `File_size` column that indicates the size of each file.
- Removed `WinMySQLAdmin` from the source distribution and from the “No Installer” Windows distribution (it had already been removed from the “With Installer” distribution before).
- The behavior of the `Last_query_cost` system variable has been changed. The default value is now 0 (rather than -1) and it now has session-level scope (rather than being global). See [Server Status Variables](#), for additional information.
- Removed `mysqlshutdown.exe` and `mysqlwatch.exe` from the Windows “No Installer” distribution (they had already been removed from the “With Installer” distribution before). Removed those programs from the source distribution.

Bugs Fixed

- MySQL would pass an incorrect key length to storage engines for `MIN()`. This could cause spurious warnings such as `InnoDB: Warning: using a partial-field key prefix in search` to appear in the `.err` log. (Bug #13218, Bug #11039)
- Build failures occurred when compiling the server on Windows using Visual Studio 6. (Bug #11153)
- Corrected a problem where an incorrect data type was returned in the result set metadata when using a prepared `SELECT DISTINCT` statement to select from a view. (Bug #11111)
- The server could crash due to an attempt to allocate too much memory when `GROUP BY blob_col` and `COUNT(DISTINCT)` were used. (Bug #11088)
- Multiple-row `REPLACE` could fail on a duplicate-key error when having one `AUTO_INCREMENT` key and one unique key. (Bug #11080)
- **InnoDB:** A duplicate key error occurred with `REPLACE` in a table having an `AUTO_INCREMENT` column. (Bug #11005)

- `WITH ROLLUP` did not sum values properly. (Bug #10982)
- **Security update:** A user with limited privileges could obtain information about the privileges of other users by querying objects in the `INFORMATION_SCHEMA` database for which that user did not have the requisite privileges. (Bug #10964)
- The value returned by the `FIELD()` function was incorrect when its parameter list contained one or more instances of `NULL`. (Bug #10944)
- Failure of a `BEFORE` trigger did not prevent the triggering statement from performing its operation on the row for which the trigger error occurred. Now the triggering statement fails as described in [Using Triggers](#). (Bug #10902)
- The `FEDERATED` storage engine properly handled outer joins, but not inner joins. (Bug #10848)
- Executing `LOAD INDEX INTO CACHE` for a table while other threads were selecting from the table caused a deadlock. (Bug #10602)
- The `TIME_FORMAT()` function returned incorrect results with some format specifiers. See [Date and Time Functions](#). (Bug #10590)
- The `LAST_DAY()` failed to return `NULL` when supplied with an invalid argument. See [Date and Time Functions](#). (Bug #10568)
- A problem with the `my_global.h` file caused compilation of MySQL to fail on single-processor Linux systems running 2.6 kernels. (Bug #10364)
- Corrected inappropriate error messages that were displayed when attempting to set the read-only `warning_count` and `error_count` system variables. (Bug #10339)
- The MySQL Instance manager caused the version to be displayed as `unknown` by `SHOW INSTANCE STATUS`. (Bug #10229)
- A simultaneous `CREATE TABLE ... SELECT FROM table` and `ALTER TABLE table` on the same table caused the server to crash. (Bug #10224)
- Under certain rare circumstances, inserting into the `mysql.host` table could cause the server to crash. (Bug #10181)
- Consistently report `INFORMATION_SCHEMA` table names in uppercase in `SHOW TABLE STATUS` output. (Bug #10059)
- Accessing `InnoDB` tables within stored functions caused the MySQL server to crash. Now, statements that perform an implicit or explicit commit or rollback are prohibited within stored functions or triggers. (Bug #10015)
- Issuing a write lock for a table from one client prevented other clients from accessing the table's metadata. For example, if one client issued a `LOCK TABLES mydb.mytable WRITE`, then a second client attempting to execute a `USE mydb;` would hang. (Bug #9998)
- Dropping stored routines when the MySQL server had been started with `--skip-grant-tables` generated extraneous warnings. (Bug #9993)
- The `mysql_next_result()` function could hang if you were executing many statements in a `mysql_real_query()` call and one of those statements raised an error. (Bug #9992)
- The functions `COALESCE()`, `IF()`, and `IFNULL()` performed incorrect conversions of their arguments. (Bug #9939)

- An incorrect result was returned from a view that selected a `COALESCE()` expression from the result of an outer join. (Bug #9938)
- **InnoDB**: Do very fast shutdown only if `innodb_fast_shutdown = 2`, but wait for threads to exit and release allocated memory if `innodb_fast_shutdown = 1`. Starting with MySQL/InnoDB 5.0.5, **InnoDB** would do brutal shutdown also when `innodb_fast_shutdown = 1`. (Bug #9673)
- Using `ORDER BY` to sort the results of an `IF()` that contained a `FROM_UNIXTIME()` expression returned incorrect results due to integer overflow. (Bug #9669)
- On Windows, with `lower_case_table_names` set to 2, using `ALTER TABLE` to alter a **MEMORY** or **InnoDB** table that had a mixed-case name also improperly changed the name to lowercase. (Bug #9660)
- The combination of `COUNT()`, `DISTINCT`, and `CONCAT()` sometimes triggered a memory deallocation bug on Windows resulting in a server crash. (Bug #9593)
- `INSERT BEFORE` triggers were not being activated for implicit inserts (`LOAD DATA`). (Bug #8755)
- The `ucs2_turkish_ci` collation failed with `upper('i')`. `UPPER/LOWER` now can return a string with different length. (Bug #8610)
- The server timed out SSL connections too quickly on Windows. (Bug #8572)
- If a stored function contained a `FLUSH` statement, the function crashed when invoked. `FLUSH` is no longer permitted within stored functions. (Bug #8409)
- `OPTIMIZE` run on an **InnoDB** table did not return a `Table is full` error if there was insufficient room in the tablespace. (Bug #8135)
- An incorrect result was obtained for columns that included an aggregate function as part of an expression, and when `WITH ROLLUP` was used with `GROUP BY`. (Bug #7914)
- Queries with `ROLLUP` returned wrong results for expressions containing `GROUP BY` columns. (Bug #7894)
- The second invocation of a stored procedure that selected from a view defined as a join using `ON` in the join condition could cause the server to crash. (Bug #6866)
- `INSERT BEFORE` triggers were not being activated for `INSERT ... SELECT` statements. (Bug #6812)
- `INSERT` or `UPDATE` when the `WHERE` clause contained a correlated subquery that referred to a column of the table being modified caused the server to crash. (Bug #6384)
- MySQL was adding a `DEFAULT` clause to `ENUM` columns that included no explicit `DEFAULT` and were defined as `NOT NULL`. (This is supposed to happen only for columns that are `NULL`.) (Bug #6267)
- Using `ALTER TABLE` for a table that had a trigger caused a crash when executing a statement that activated the trigger, and also a crash later with `USE db_name` for the database containing the table. (Bug #5894)
- Triggers with dropped functions caused crashes. (Bug #5893)
- Triggers were not being activated for multiple-table `UPDATE` or `DELETE` statements. (Bug #5860)
- The incorrect sequence of statements `HANDLER tbl_name READ index_name NEXT` without a preceding `HANDLER tbl_name READ index_name = (value_list)` for an **InnoDB** table resulted in a server crash rather than an error. (Bug #5373)

- Multiple-table `DELETE` always deleted on the fly from the first table that was to be deleted from. In some cases, when using many tables and when necessary to access the same row twice in the first table, some rows to be deleted from other tables could be missed.

Changes in MySQL 5.0.6 (2005-05-26)

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- **Incompatible Change:** The behavior of `LOAD DATA INFILE` and `SELECT ... INTO OUTFILE` has changed when the `FIELDS TERMINATED BY` and `FIELDS ENCLOSED BY` values both are empty. Formerly, a column was read or written the display width of the column. For example, `INT(4)` was read or written using a field with a width of 4. Now columns are read and written using a field width wide enough to hold all values in the field. However, data files written before this change was made might not be reloaded correctly with `LOAD DATA INFILE` for MySQL 4.1.12 and up. This change also affects data files read by `mysqlimport` and written by `mysqldump --tab`, which use `LOAD DATA INFILE` and `SELECT ... INTO OUTFILE`. For more information, see [LOAD DATA INFILE Syntax](#). (Bug #12564)
- **Incompatible Change:** `MyISAM` and `InnoDB` tables created with `DECIMAL` columns in MySQL 5.0.3 to 5.0.5 will appear corrupt after an upgrade to MySQL 5.0.6. Dump such tables with `mysqldump` before upgrading, and then reload them after upgrading. (The same incompatibility will occur for these tables created in MySQL 5.0.6 after a downgrade to MySQL 5.0.3 to 5.0.5.) (Bug #10465, Bug #10625)
- When the server cannot read a table because it cannot read the `.frm` file, print a message that the table was created with a different version of MySQL. (This can happen if you create tables that use new features and then downgrade to an older version of MySQL.) (Bug #10435)
- The `GRANT` and `REVOKE` statements now support an `object_type` clause to be used for disambiguating whether the grant object is a table, a stored procedure, or a stored function. Use of this clause requires that you upgrade your grant tables. See [mysql_fix_privilege_tables — Upgrade MySQL System Tables](#). (Bug #10246)
- Added `REFERENCED_TABLE_SCHEMA`, `REFERENCED_TABLE_NAME`, and `REFERENCED_COLUMN_NAME` columns to the `KEY_COLUMN_USAGE` table of `INFORMATION_SCHEMA`. (Bug #9587)
- The use of `SESSION` or `GLOBAL` for user variables, or for local variables in stored routines, is no longer permitted. (Bug #9286)
- New `/*>` prompt for `mysql`. This prompt indicates that a `/* ... */` comment was begun on an earlier line and the closing `*/` sequence has not yet been seen. (Bug #9186)
- The `INFORMATION_SCHEMA.SCHEMATA` table now has a `DEFAULT_COLLATION_NAME` column. (Bug #8998)
- Added a `--show-warnings` option to `mysql` to cause warnings to be shown after each statement if there are any. This option applies to interactive and batch mode. In interactive mode, `\w` and `\W` may be used to enable and disable warning display. (Bug #8684)
- If strict SQL mode is enabled, `VARCHAR` and `VARBINARY` columns with a length greater than 65,535 no longer are silently converted to `TEXT` or `BLOB` columns. Instead, an error occurs. (Bug #8295, Bug #8296)
- Removed a limitation that prevented use of FIFOs as logging targets (such as for the general query log). This modification *does not apply* to the binary log and the relay log. (Bug #8271)

- `SHOW VARIABLES` now shows the `slave_compressed_protocol`, `slave_load_tmpdir` and `slave_skip_errors` system variables. (Bug #7800)
- **InnoDB**: When the maximum length of `SHOW INNODB STATUS` output would be exceeded, truncate the beginning of the list of active transactions, instead of truncating the end of the output. (Bug #5436)
- **InnoDB**: If `innodb_locks_unsafe_for_binlog` is enabled and the isolation level of the transaction is not set to `SERIALIZABLE`, **InnoDB** uses a consistent read for select in clauses such as `INSERT INTO ... SELECT` and `UPDATE ... (SELECT)` that do not specify `FOR UPDATE` or `LOCK IN SHARE MODE`. Thus, no locks are set to rows read from selected table.
- Added the `div_precision_increment` system variable, which indicates the number of digits by which to increase the scale of the result of division operations performed with the `/` operator.
- Removed `mysqlshutdown.exe` and `mysqlwatch.exe` from the Windows “With Installer” distribution.
- The precision of the `DECIMAL` data type has been increased from 64 to 65 decimal digits.
- Added the `--log-bin-trust-routine-creators` server option for setting the `log_bin_trust_routine_creators` system variable from the command line.
- Updated version of `libedit` to 2.9. (Bug #2596)
- Implemented the `STMT_ATTR_PREFETCH_ROWS` option for the `mysql_stmt_attr_set()` C API function. This sets how many rows to fetch at a time when using cursors with prepared statements.
- Added the `log_bin_trust_routine_creators` system variable, which applies when binary logging is enabled. It controls whether stored routine creators can be trusted not to create stored routines that will cause unsafe events to be written to the binary log.
- Removed unused system variable `myisam_max_extra_sort_file_size`.
- Changed default value of `myisam_data_pointer_size` from 4 to 6. This enables us to avoid `table is full` errors for most cases.
- Added a `--debug` option to `my_print_defaults`.
- The variable `concurrent_insert` now takes 3 values. Setting this to 2 changes **MyISAM** to do concurrent inserts to end of table if table is in use by another thread.

Bugs Fixed

- **Security Fix**: `mysql_install_db` created the `mysql_install_db.x` file with a predictable file name and insecure permissions, which permitted local users to execute arbitrary SQL statements by modifying the file's contents. (CVE-2005-1636)
- **Replication**: Statements that create and drop triggers were not being written to the binary log, which affects replication and data recovery options. Trigger-related statements now are logged, subject to the issues and limitations discussed in [Binary Logging of Stored Programs](#). (Bug #10417)
- **Replication**: Statements that create and use stored routines were not being written to the binary log, which affects replication and data recovery options. Stored routine-related statements now are logged, subject to the issues and limitations discussed in [Binary Logging of Stored Programs](#). (Bug #2610)
- **MERGE** tables could fail on Windows due to incorrect interpretation of path name separator characters for file names in the `.MRG` file. (Bug #10687)
- Repeated calls to `ABS()` when the argument evaluated to `NULL` crashed the server. (Bug #10599)

- `SELECT 0/0` returned `0` rather than `NULL`. (Bug #10404)
- `INSERT ... ON DUPLICATE KEY UPDATE` with `MERGE` tables, which do not have unique indexes, caused the server to crash. (Bug #10400)
- `AUTO_INCREMENT` in `InnoDB` tables could assign the same value for several rows. (Bug #10359)
- `mysqldump` crashed using the `--complete-insert` option while dumping tables with a large number of long column names. (Bug #10286)
- Incomplete results were returned from `INFORMATION_SCHEMA.COLUMNS` for `INFORMATION_SCHEMA` tables for non-`root` users. (Bug #10261)
- `mysql.cc` did not compile correctly using `VC++` on Windows. (Bug #10245)
- Using `#pragma interface` or `#pragma implementation` in source files caused portability issues for `cygwin`. (Bug #10241)
- Corrected a problem where `DEFAULT` values were not assigned properly to `BIT(1)` or `CHAR(1)` columns if certain other columns preceded them in the table definition. (Bug #10179)
- The `BLACKHOLE` storage engine failed in testing, causing the server to crash. (Bug #10175)
- The optimizer was choosing suboptimal execution plans for certain outer joins where the right table of a left join (or left table of a right join) had both `ON` and `WHERE` conditions. (Bug #10162)
- Corrected a problem resolving outer column references in correlated subqueries when using the prepared statements. (Bug #10041)
- `INFORMATION_SCHEMA` tables were inaccessible depending on the lettercase used to refer to them. (Bug #10018)
- `awk` script portability problems were found in `cmd-line-utils/libedit/makelist.sh`. (Bug #9954)
- The error message for exceeding `MAX_CONNECTIONS_PER_HOUR` mistakenly referred to `max_connections`. (Bug #9947)
- `RENAME TABLE` for an `ARCHIVE` table failed if the `.arn` file was not present. (Bug #9911)
- A `CHECK TABLE` statement whose arguments were a view name followed by a table name caused the server to crash. (Bug #9897)
- `my_print_defaults` was ignoring the `--defaults-extra-file` option or crashing when the option was given. (Bug #9851, Bug #9136)
- Within a stored procedure, attempting to update a view defined as an inner join failed with a `Table 'tbl_name' was locked with a READ lock and can't be updated` error. (Bug #9841)
- The `INFORMATION_SCHEMA.COLUMNS` table was missing columns of views for which the user has access. (Bug #9838)
- Use of a `CHAR` or `VARCHAR` column with `MIN()` or `MAX()` and `GROUP BY ... WITH ROLLUP` caused the server to crash. (Bug #9820)
- Use `DISTINCT AVG()` with `GROUP BY ... WITH ROLLUP` caused the server to crash. (Bug #9800)
- Using `AVG(DISTINCT)` with `GROUP BY ... WITH ROLLUP` caused the server to crash. (Bug #9799)

- Using `GROUP BY ... WITH ROLLUP` on an indexed column in an InnoDB table could cause the server to crash. (Bug #9798)
- Corrected some failures of prepared statements for SQL (`PREPARE` plus `EXECUTE`) to return all rows for some `SELECT` statements. (Bug #9777, Bug #9096)
- `CREATE TABLE ... LIKE` did not work correctly when `lower_case_table_names` was set on a case-sensitive file system and the source table name was not given in lowercase. (Bug #9761)
- Corrected an inability to select from a view within a stored procedure. (Bug #9758)
- `net_read_timeout` and `net_write_timeout` were not being respected on Windows. (Bug #9721)
- `libsupc++` was longer required for building on FreeBSD 5.3. (Bug #9714)
- The `mysql_stmt_attr_set()` C API function now returns an error for option values that are defined in `mysql.h` but not yet implemented, such as `CURSOR_TYPE_SCROLLABLE`. (Bug #9643)
- Memory block allocation did not function correctly for the query cache in the embedded server. (Bug #9549)
- `CREATE TABLE t AS SELECT UUID()` created a `VARCHAR(12)` column, which is too small to hold the 36-character result from `UUID()`. (Bug #9535)
- `SELECT DISTINCT` with a prepared statement that used a cursor could cause the server to crash. (Bug #9520)
- `NULL` key parts in hash indexes on `VARCHAR` columns were not handled correctly, resulting in incorrect query results. (Bug #9489, Bug #10176)
- The `mysql_stmt_execute()` and `mysql_stmt_reset()` C API functions now close any cursor that is open for the statement, which prevents a server crash. (Bug #9478)
- `SELECT` from `INFORMATION_SCHEMA` tables failed if the statement has a `GROUP BY` clause and an aggregate function in the select list. (Bug #9404)
- `MAX()` for an `INT UNSIGNED` (unsigned 4-byte integer) column could return negative values if the column contained values larger than 2^{31} . (Bug #9298)
- Disabled binary logging within stored routines to avoid writing spurious extra statements to the binary log. For example, if a routine `p()` executes an `INSERT` statement, then for `CALL p()`, the `CALL` statement appears in the binary log, but not the `INSERT` statement. (Bug #9100)
- `FORMAT()` now performs better rounding for double values (for example, `FORMAT(4.55,1)` returns 4.6, not 4.5). (Bug #9060)
- `SHOW CREATE VIEW` got confused and could not find the view if there was a temporary table with the same name as the view. (Bug #8921)
- Selecting from a single-table view defined on multiple-table views caused a server crash. (Bug #8528)
- Remove extra slashes in `--tmpdir` value (for example, convert `/var//tmp` to `/var/tmp`, because they caused various errors. (Bug #8497)
- Invoking a stored function that executed a `SHOW` statement resulted in a server crash. (Bug #8408)
- An error in the implementation of the MyISAM compression algorithm caused `myisampack` to fail with very large sets of data (total size of all the records in a single column needed to be at least 3 GB to trigger this issue). (Bug #8321)

- Added `Create_routine_priv`, `Alter_routine_priv`, and `Execute_priv` privileges to the `mysql.host` privilege table. (They had been added to `mysql.db` in MySQL 5.0.3 but not to the `host` table.) (Bug #8166)
- A deadlock resulted from using `FLUSH TABLES WITH READ LOCK` while an `INSERT DELAYED` statement was in progress. (Bug #7823)
- In strict SQL mode, some assignments to numeric columns that should have been rejected were not (such as the result of an arithmetic expression or an explicit `CAST()` operation). (Bug #6961)
- For `MERGE` tables, avoid writing absolute path names in the `.MRG` file for the names of the constituent `MyISAM` tables so that if the data directory is moved, `MERGE` tables will not break. For `mysqld`, write just the `MyISAM` table name if it is in the same database as the `MERGE` table, and a path relative to the data directory otherwise. For the embedded servers, absolute path names may still be used. (Bug #5964)
- Multiple calls to a stored procedure that assigned the result of a subquery to a variable or compared it to a value with `IN` could cause the server to crash. (Bug #5963)
- If the file named by a `--defaults-extra-file` option does not exist or is otherwise inaccessible, an error now occurs. (Bug #5056)
- `configure` did not properly recognize whether NPTL was available on Linux. (Bug #2173)

Changes in MySQL 5.0.5 (Not released)

No public release of MySQL 5.0.5 was made. The changes described in this section are available in MySQL 5.0.6.

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- **MySQL Cluster:** More informative error messages are provided when a query is issued against an `NDB` table that has been modified by another `mysqld` server. (Bug #6762)
- **InnoDB:** When `foreign_key_checks = 0`, `ALTER TABLE` and `RENAME TABLE` will ignore any type incompatibilities between referencing and referenced columns. Thus, it will be possible to convert the character sets of columns that participate in a foreign key. Be sure to convert all tables before modifying any data! (Bug #9802)
- `SHOW VARIABLES` no longer displays the deprecated `log_update` system variable. (Bug #9738)
- Added support for the `BIT` data type to the `MEMORY`, `InnoDB`, and `BDB` storage engines.
- The behavior controlled by the `--innodb-fast-shutdown` option now can be changed at runtime by setting the value of the global `innodb_fast_shutdown` system variable. It now accepts values 0, 1 and 2 (except on Netware where 2 is disabled). If set to 2, then when the MySQL server shuts down, `InnoDB` will just flush its logs and shut down brutally (and quickly) as if a MySQL crash had occurred; no committed transaction will be lost, but a crash recovery will be done at next startup.

Bugs Fixed

- **Security Fix:** Starting `mysqld` with `--user=non_existent_user` caused it to run using the privileges of the account from which it was invoked, including the `root` account. (Bug #9833)
- A memory leak occurred when selecting from a view that contained a subquery. (Bug #10107)

- Setting the `storage_engine` system variable to `MEMORY` succeeded, but retrieving the variable resulted in a value of `HEAP` (the old name for the `MEMORY` storage engine) rather than `MEMORY`. (Bug #10039)
- Queries containing `CURRENT_USER()` incorrectly were registered in the query cache. (Bug #9796)
- Invoking a stored function that returned a value having an `ENUM` or `SET` data type caused the server to crash. (Bug #9775)
- A string length comparison problem caused `mysql` to fail when loading dump files containing certain escape sequences containing a backslash character (`\`). (Bug #9756)
- After an internal temporary table became too large in memory and had to be converted to an on-disk table, the error indicator was not cleared and the query failed with error 1023 `Can't find record in ''`. (Bug #9703)
- Use of a subquery that used `WITH ROLLUP` in the `FROM` clause of the main query sometimes resulted in a `Column cannot be null` error. (Bug #9681)
- **InnoDB**: Assertion failures of types `ut_a(cursor->old_stored == BTR_PCUR_OLD_STORED)` and `prebuilt->template_type == 0` could occur when performing multi-table updates. This bug was introduced in 4.1.10 and 4.0.24. (Bug #9670)
- A problem with `readline` caused the `mysql` client to crash when the user pressed **Control+R**. (Bug #9568)
- Executing `LOCK TABLES` and then calling a stored procedure caused an error and resulting in the server thinking that no stored procedures exist. (Bug #9566)
- The server died with signal 11 if a nonexistent location was specified for the location of the binary log. Now the server exits after printing an appropriate error message. (Bug #9542)
- Incorrect results were returned for queries of the form `SELECT ... LEFT JOIN ... WHERE EXISTS (subquery)`, where the subquery selected rows based on an `IS NULL` condition. (Bug #9516)
- A segmentation fault in `mysqlcheck` occurred when the last table checked in `--auto-repair` mode returned an error (such as the table being a `MERGE` table). (Bug #9492)
- Within a stored procedure, attempting to execute a multiple-table `UPDATE` failed with a `Table 'tbl_name' was locked with a READ lock and can't be updated` error. (Bug #9486)
- `mysqlshow` displayed an incorrect row count for tables. (Bug #9391)
- **InnoDB**: Next-key locking did not permit inserts which did not produce a “phantom”. If the range is of type `'a' <= uniquecolumn`, **InnoDB** lock only the RECORD, if the record with the column value `'a'` exists in a `CLUSTERED` index. This enables inserts before a range. (Bug #9354)
- The optimizer did not compute the union of two ranges for the `OR` operator correctly. (Bug #9348)
- Corrected a failure to resolve a column reference correctly for a `LEFT JOIN` that compared a join column to an `IN` subquery. (Bug #9338)
- `OPTIMIZE TABLE` was written twice to the binary log when used on **InnoDB** tables. (Bug #9149)
- Multiple-table updates could produce spurious data-truncation warnings if they used a join across columns that are indexed using a column prefix. (Bug #9103)
- Invocation of a stored function that returned a value having a `BLOB` data type caused the server to crash. (Bug #9102)

- For stored functions that should return a [YEAR](#) value, corrected a failure of the value to be in [YEAR](#) format. (Bug #8861)
- Selecting from a view containing a subquery caused the server to hang. (Bug #8490)
- [TIMEDIFF\(\)](#) with a negative time first argument and positive time second argument produced incorrect results. (Bug #8068)
- Invocation of a stored function that returned a value having a [BIT](#) data type caused the server to crash. (Bug #7648)
- [SET @var= CAST\(NULL AS \[INTEGER|CHAR\]\)](#) now sets the result type of the variable to [INTEGER/CHAR](#). (Bug #6598)
- The client/server protocol permitted the server to close the connection before sending the final error message. The problem could show up as a [Lost connection to MySQL server](#) error during a query when attempting to connect and access a nonexistent database. (Bug #6387, Bug #9455)
- Column references were not properly resolved when an outer join involving a view contained a subquery and the column was used both in the subquery and the outer query. (Bug #6107, Bug #6106)
- [InnoDB](#): Prevent [ALTER TABLE](#) from changing the storage engine if there are foreign key constraints on the table. (Bug #5574, Bug #5670)

Changes in MySQL 5.0.4 (2005-04-16)

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- **Replication:** The way the time zone information is stored in the binary log was changed, so that it is now possible to have a replication master and slave running with different global time zones. A disadvantage is that replication from 5.0.4 masters to pre-5.0.4 slaves is impossible.
- Added [ENGINE=MyISAM](#) table option when creating [mysql.proc](#) table in [mysql_create_system_tables](#) script to make sure the table is created as a [MyISAM](#) table even if the default storage engine has been changed. (Bug #9496)
- [SHOW CREATE TABLE](#) for an [INFORMATION_SCHEMA](#) table no longer prints a [MAX_ROWS](#) value because the value has no meaning. (Bug #8941)
- Support for MIT-pthreads was removed.
- Invalid [DEFAULT](#) values for [CREATE TABLE](#) now generate errors. (Bug #5903)
- Added [--show-table-type](#) option to [mysqlshow](#), to display a column indicating the table type, as in [SHOW FULL TABLES](#). (Bug #5036)
- New configuration directives [!include](#) and [!includedir](#) implemented for including option files and searching directories for option files. See [Using Option Files](#), for usage.
- Added [--with-big-tables](#) compilation option to [configure](#). (Previously it was necessary to pass [-DBIG_TABLES](#) to the compiler manually to enable large table support.) See [MySQL Source-Configuration Options](#), for details.

Bugs Fixed

- **Security Fix:** Information in `INFORMATION_SCHEMA` could be exposed to a user with insufficient privileges. (Bug #7214)
- **MySQL Cluster:** The commit count cache for `NDB` was not properly invalidated when deleting a record using a cursor. (Bug #8585)
- **Replication:** If, on a replication master, a `LOAD DATA INFILE` operation was interrupted (by, for example, an integrity constraint violation or killed connection), the slave skipped the `LOAD DATA INFILE` entirely, thus missing changes if this command permanently inserted or updated table records before being interrupted. (Bug #3247)
- `mysql.server` no longer uses nonportable `alias` command or LSB functions. (Bug #9852)
- A server installed as a Windows service and started with `--shared-memory` could not be stopped. (Bug #9665)
- Selecting a `BIT` column failed if the binary client/server protocol was used. (Bug #9608)
- Creating a `PRIMARY KEY` on a table having a `BIT` column caused the server to crash. (Bug #9571)
- `ENUM` and `SET` columns in `InnoDB` tables were treated incorrectly as character strings. This bug did not manifest itself with `latin1` collations, but it caused malfunction with `utf8`. Old tables will continue to work. In new tables, `ENUM` and `SET` will be stored internally as unsigned integers. (Bug #9526)
- An error in division of floating point numbers could cause nine zeros (`000000000`) to be inserted in the middle of the quotient. (Bug #9501)
- Fixed option-parsing code for the embedded server to understand `K`, `M`, and `G` suffixes for the `net_buffer_length` and `max_allowed_packet` options. (Bug #9472)
- Some user variables were not being handled with “implicit” coercibility. (Bug #9425)
- Using `CREATE TABLE ... SELECT` or `INSERT INTO ... SELECT` to select from multiple-table view caused the server to crash. (Bug #9398, Bug #8703)
- Multiple executions of a prepared statement involving a join of an `INFORMATION_SCHEMA` table with another table could lead to a crash of the server. (Bug #9383)
- An `InnoDB` test suite failure was caused by a locking conflict between two server instances at server shutdown or startup. This conflict on advisory locks appears to be the result of a bug in the operating system; these locks should be released when the files are closed, but somehow that does not always happen immediately in Linux. (Bug #9381)
- Permit extra HKSCS and cp950 characters (`big5` extension characters) to be accepted in `big5` columns. (Bug #9357)
- The value of the `CHARACTER_MAXIMUM_LENGTH` and `CHARACTER_OCTET_LENGTH` columns of the `INFORMATION_SCHEMA.COLUMNS` table must be `NULL` for numeric columns, but were not. (Bug #9344)
- `INFORMATION_SCHEMA` tables had an implicit upper limit for the number of rows. As a result, not all data could be returned for some queries. (Bug #9317)
- `InnoDB`: True `VARCHAR`: `InnoDB` stored the 'position' of a row wrong in a column prefix primary key index; this could cause MySQL to complain `ERROR 1032: Can't find record ...` in an update of the primary key, and also some `ORDER BY` or `DISTINCT` queries. (Bug #9314)
- `ORDER BY` sometimes caused incorrect sorting of `UTF8` data. (Bug #9309)

- The `utf8_spanish2_ci` and `ucs2_spanish2_ci` collations no longer consider `r` equal to `rr`. If you upgrade to this version from an earlier version, you should rebuild the indexes of any affected tables. (Bug #9269)
- `CREATE OR REPLACE VIEW` and `ALTER VIEW` now require the `CREATE VIEW` and `DROP` privileges, not `CREATE VIEW` and `DELETE`. (`DELETE` is a row-level privilege, not a table-level privilege.) (Bug #9260)
- Using `GROUP BY` on a decimal expression caused the server to crash. (Bug #9210)
- `mysqldump` dumped core when invoked with `--tmp` and `--single-transaction` options and a nonexistent table name. (Bug #9175)
- Calling `mysql_stmt_close()` for a single-row result set could cause the server to crash. (Bug #9159)
- Setting the `max_error_count` system variable to 0 resulted in a setting of 1. (Bug #9072)
- The use of `XOR` together with `NOT ISNULL()` erroneously resulted in some outer joins being converted to inner joins by the optimizer. (Bug #9017)
- Two prepared statements for single-row result sets being open simultaneously caused a `Commands out of sync error`. (Bug #8880)
- Extraneous comparisons between `NULL` values in indexed columns were performed by the optimizer for operators such as `=` that are never true for `NULL`. (Bug #8877)
- In the client/server protocol for prepared statements, reconnection failed when the connection was killed with reconnection enabled. (Bug #8866)
- In prepared statements, subqueries containing parameters were erroneously treated as `const` tables during preparation, resulting in a server crash. (Bug #8807)
- Do not try to space-pad `BLOB` columns containing `ucs2` characters. (Bug #8771)

References: This issue is a regression of: Bug #7350.

- The warning message from `GROUP_CONCAT()` did not always indicate the correct number of lines. (Bug #8681)
- `InnoDB`: SQL statements were not rolled back on error. (Bug #8650)
- Too many rows were returned from queries that combined `ROLLUP` and `LIMIT` if `SQL_CALC_FOUND_ROWS` was given. (Bug #8617)
- Incorrect results were returned from queries that combined `SELECT DISTINCT`, `GROUP BY`, and `ROLLUP`. (Bug #8616)
- Queries that combined `SELECT DISTINCT`, `SUM()`, and `ROLLUP` could cause the MySQL server to crash. (Bug #8615)
- The `tee` command could sometimes cause the `mysql` client to crash. (Bug #8499)
- `DROP TABLE` did not drop triggers that were defined for the table. `DROP DATABASE` did not drop triggers in the database. (Bug #6559, Bug #5859)
- Added linking with `libsupc++` on Fedora Core 3 to get language support functions. (Bug #6554)
- Unions between binary and nonbinary columns failed due to a collation coercibility problem. (Bug #6519)

- Using `CONVERT('0000-00-00',DATE)` or `CAST('0000-00-00' as DATE)` with the `NO_ZERO_DATE` SQL mode enabled now produces a warning. (Bug #6145)
- `TRADITIONAL` SQL mode should prevent inserts where a column with no default value is omitted or set to a value of `DEFAULT`; however, in some cases, this restriction was not enforced. (Bug #5986)
- Inserting a zero date in a `DATE`, `DATETIME` or `TIMESTAMP` column during `TRADITIONAL` mode now produces an error. (Bug #5933)
- `CAST()` now produces warnings when casting incorrect `INTEGER` and `CHAR` values. This also applies to implicit `string` to `number` casts. (Bug #5912)
- An error now occurs if you try to insert an invalid value using a stored procedure in `STRICT` mode. (Bug #5907)
- `STR_TO_DATE()` now produces errors in strict mode (and warnings otherwise) when given an illegal argument. (Bug #5902)
- Inserting a zero date into a `DATETIME` column in `TRADITIONAL` mode now produces an error.
- `ALTER TABLE` now fails in `STRICT` mode if the alteration generates warnings.

Changes in MySQL 5.0.3 (2005-03-23, Beta)



Note

This Beta release, as any other pre-production release, should not be installed on “production” level systems or systems with critical data. It is good practice to back up your data before installing any new version of software. Although MySQL worked very hard to ensure a high level of quality, protect your data by making a backup as you would for any software beta release.

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- **Incompatible Change:** The C API `ER_WARN_DATA_TRUNCATED` warning symbol was renamed to `WARN_DATA_TRUNCATED`.
- **Incompatible Change:** The `DECIMAL` and `NUMERIC` data types now are handled with a fixed-point library that enables precision math handling that results in more accurate results. See [Precision Math](#).

A consequence of the change in handling of the `DECIMAL` and `NUMERIC` fixed-point data types is that the server is more strict to follow standard SQL. For example, a data type of `DECIMAL(3,1)` stores a maximum value of 99.9. Previously, the server permitted larger numbers to be stored. That is, it stored a value such as 100.0 as 100.0. Now the server clips 100.0 to the maximum permissible value of 99.9. If you have tables that were created before MySQL 5.0.3 and that contain floating-point data not strictly legal for the data type, you should alter the data types of those columns. For example:

```
ALTER TABLE tbl_name MODIFY col_name DECIMAL(4,1);
```

For user-defined functions, exact-value decimal arguments such as `1.3` or `DECIMAL` column values were passed as `REAL_RESULT` values prior to MySQL 5.0.3. As of 5.0.3, they are passed as strings with a type of `DECIMAL_RESULT`. If you upgrade to 5.0.3 and find that your UDF now receives string

values, use the initialization function to coerce the arguments to numbers as described in [UDF Argument Processing](#).

For the [FLOOR\(\)](#) and [CEILING\(\)](#) functions, the return type is no longer always [BIGINT](#). For exact-value numeric arguments, the return value has an exact-value numeric type. For string or floating-point arguments, the return value has a floating-point type.

- **MySQL Cluster; Replication:** Added a new global system variable [slave_transaction_retries](#): If the replication slave SQL thread fails to execute a transaction because of an [InnoDB](#) deadlock or exceeded [InnoDB's innodb_lock_wait_timeout](#) or [NDBCLUSTER's TransactionDeadlockDetectionTimeout](#) or [TransactionInactiveTimeout](#), it automatically retries [slave_transaction_retries](#) times before stopping with an error. The default is 10. (Bug #8325)
- **MySQL Cluster:** When using this storage engine, the output of [SHOW TABLE STATUS](#) now displays properly calculated values in the [Avg_row_length](#) and [Data_length](#) columns. (Note that [BLOB](#) columns are not yet taken into account.) In addition, the number of replicas is now shown in the [Comment](#) column (as [number_of_replicas](#)).
- **Replication:** The [LOAD DATA](#) statement was extended to support user variables in the target column list, and an optional [SET](#) clause. Now one can perform some transformations on data after they have been read and before they are inserted into the table. For example:

```
LOAD DATA INFILE 'file.txt'  
INTO TABLE t1  
(column1, @var1)  
SET column2 = @var1/100;
```

Also, replication of [LOAD DATA](#) was changed, so you can't replicate such statements from a 5.0.3 master to pre-5.0.3 slaves.

- **Replication:** The way the character set information is stored into the binary log was changed, so that it is now possible to have a replication master and slave running with different global character sets. A disadvantage is that replication from 5.0.3 masters to pre-5.0.3 slaves is impossible.
- **Replication:** If the MySQL server is started without an argument to [--log-bin](#) and without [--log-bin-index](#), thus not providing a name for the binary log index file, a warning is issued because MySQL falls back to using the host name for that name, and this is prone to replication issues if the server's host name gets changed later.
- Nonoptimal [index_merge](#) query execution plans were chosen on IRIX. (Bug #8578)
- [mysqld_safe](#) will create the directory where the UNIX socket file is to be located if the directory does not exist. This applies only to the last component of the directory path name. (Bug #8513)
- [ONLY_FULL_GROUP_BY](#) no longer is included in the [ANSI](#) composite SQL mode. (Bug #8510)
- The server now includes a timestamp in the [Ready for connections](#) message that is written to the error log at startup. (Bug #8444)
- [CHECKSUM TABLE](#) returns a warning for nonexisting tables. The checksum value remains [NULL](#) as before. (Bug #8256)
- Setting the connection collation to a value different from the server collation followed by a [CREATE TABLE](#) statement that included a quoted default value resulted in a server crash. (Bug #8235)
- When a client releases a user-level lock, [DO RELEASE_LOCK\(\)](#) will not be written to the binary log anymore (this makes the binary log smaller); as a counterpart, the slave does not actually take the lock

when it executes `GET_LOCK()`. This is mainly an optimization and should not affect existing setups. (Bug #7998)

- **InnoDB**: Corrected a bug in the crash recovery of `ROW_FORMAT=COMPACT` tables that caused corruption. There may still be bugs in the crash recovery, especially in `COMPACT` tables. (Bug #7973)
- Permitted the service-installation command for Windows servers to specify a single option other than `--defaults-file` following the service name. This is for compatibility with MySQL 4.1. (Bug #7856)
- Changed XML format for `mysql` from `<col_name>col_value</col_name>` to `<field name="col_name">col_value</field>` to enable proper encoding of column names that are not legal as element names. (Bug #7811)
- `SHOW CREATE TABLE` now uses `USING index_type` rather than `TYPE index_type` to specify an index type. (Bug #7233)
- **InnoDB**: Implemented fast `TRUNCATE TABLE`. The old approach (deleting rows one by one) may be used if the table is being referenced by foreign keys. (Bug #7150)
- Out-of-order packets were sent (`ERROR` after `OK` or `EOF`) following a `KILL QUERY` statement. (Bug #6804)
- Added `sql_notes` session variable to cause `Note`-level warnings not to be recorded. (Bug #6662)
- Added `mysql_library_init()` and `mysql_library_end()` as synonyms for the `mysql_server_init()` and `mysql_server_end()` C API functions. `mysql_library_init()` and `mysql_library_end()` are `#define` symbols, but the names more clearly indicate that they should be called when beginning and ending use of a MySQL C API library no matter whether the application uses `libmysqlclient` or `libmysqld`. (Bug #6149)
- **InnoDB**: A commit is now performed after every 10,000 copied rows when executing `ALTER TABLE`, `CREATE INDEX`, `DROP INDEX` or `OPTIMIZE TABLE`. This makes recovery from an aborted operations of these types much faster than previous to this change.
- Added support for `AVG(DISTINCT)`.
- A new `CREATE USER` privilege was added.
- Support for `RAID` options in `MyISAM` tables has been removed. If you have tables that use these options, you should convert them before upgrading. See [Changes Affecting Upgrades to 5.0](#).
- **InnoDB**: A shared record lock (`LOCK_REC_NOT_GAP`) is now taken for a matching record in the foreign key check because inserts can be permitted into gaps.
- The MySQL server now aborts when started with the option `--log-bin-index` and without `--log-bin`, and when started with `--log-slave-updates` and without `--log-bin`.
- API change: the `reconnect` flag in the `MYSQL` structure is now set to 0 by `mysql_real_connect()`. Only those client programs which didn't explicitly set this flag to 0 or 1 after `mysql_real_connect()` experience a change. Having automatic reconnection enabled by default was considered too dangerous (after reconnection, table locks, temporary tables, user and session variables are lost).
- Bit-field values can be written using `b'value'` notation. `value` is a binary value written using 0s and 1s.
- **InnoDB**: Relaxed locking in `INSERT ... SELECT`, single table `UPDATE ... (SELECT)` and single table `DELETE ... (SELECT)` clauses when `innodb_locks_unsafe_for_binlog` is used and isolation level of the transaction is not `SERIALIZABLE`. **InnoDB** uses consistent read in these cases for a selected table.

- **InnoDB** now supports a fast `TRUNCATE TABLE`. One visible change from this is that auto-increment values for this table are reset on `TRUNCATE TABLE`.
- **InnoDB**: Introduced a compact record format that does not store the number of columns or the lengths of fixed-size columns. The old format can be requested by specifying `ROW_FORMAT=REDUNDANT`. The new format (`ROW_FORMAT=COMPACT`) is the default. The new format typically saves 20% of disk space and memory.

The presence of the new compact row format decreases row storage space by about 20% at the cost of increasing CPU use for some operations. If your workload is a typical one that is limited by cache hit rates and disk speed it is likely to be faster. If it is a rare case that is limited by CPU speed, it might be slower.

- From the Windows distribution, predefined accounts without passwords for remote users (`'root'@'%'`, `' '@' %'`) were removed (other distributions never had them).
- Added the `FEDERATED` storage engine. See [The FEDERATED Storage Engine](#).
- User variable coercibility has been changed from “coercible” to “implicit.” That is, user variables have the same coercibility as column values.
- Security improvement: User-defined functions should have at least one symbol defined in addition to the `xxx` symbol that corresponds to the main `xxx()` function. These auxiliary symbols correspond to the `xxx_init()`, `xxx_deinit()`, `xxx_reset()`, `xxx_clear()`, and `xxx_add()` functions. `mysqld` by default no longer loads UDFs unless they have at least one auxiliary symbol defined in addition to the main symbol. The `--allow-suspicious-udfs` option controls whether UDFs that have only an `xxx` symbol can be loaded. By default, the option is off. `mysqld` also checks UDF file names when it reads them from the `mysql.func` table and rejects those that contain directory path name separator characters. (It already checked names as given in `CREATE FUNCTION` statements.) See [UDF Calling Sequences for Simple Functions](#), [UDF Calling Sequences for Aggregate Functions](#), and [UDF Security Precautions](#). Thanks to Stefano Di Paola <stefano.dipaola@wisec.it> for finding and informing us about this issue. (CVE-2005-0709, CVE-2005-0710)
- Added the `--large-pages` option for `mysqld`. Large page support can be used on Linux systems. See [Enabling Large Page Support](#).
- Added an `error` member to the `MYSQL_BIND` data structure that is used in the C API for prepared statements. This member is used for reporting data truncation errors. Truncation reporting is enabled using the new `MYSQL_REPORT_DATA_TRUNCATION` option for the `mysql_options()` C API function.
- Added `VAR_POP()` and `STDDEV_POP()` as standard SQL aliases for the `VARIANCE()` and `STDDEV()` functions that compute population variance and standard deviation. Added new `VAR_SAMP()` and `STDDEV_SAMP()` functions to compute sample variance and standard deviation. (Bug #3190)
- Added the `multi_range_count` system variable.
- The coercibility for the return value of functions such as `USER()` or `VERSION()` now is “system constant” rather than “implicit.” This makes these functions more coercible than column values so that comparisons of the two do not result in `Illegal mix of collations` errors. `COERCIBILITY()` was modified to accommodate this new coercibility value. See [Information Functions](#).
- **InnoDB: Upgrading from 4.1:** The sorting order for end-space in `TEXT` columns for **InnoDB** tables has changed. Starting from 5.0.3, **InnoDB** compares `TEXT` columns as space-padded at the end. If you have a nonunique index on a `TEXT` column, you should run `CHECK TABLE` on it, and run `OPTIMIZE TABLE` if the check reports errors. If you have a `UNIQUE INDEX` on a `TEXT` column, you should rebuild the table with `OPTIMIZE TABLE`.

- Boolean full-text phrase searching now requires only that matches contain exactly the same words as the phrase and in the same order. Nonword characters no longer need match exactly.
- `my.cnf` in the compile-time datadir (usually `/usr/local/mysql/data/` in the binary tarball distributions) is not being read anymore. The value of the environment variable `MYSQL_HOME` is used instead of the hard-coded path.
- Additional control over transaction completion was implemented. The `COMMIT` and `ROLLBACK` statements support `AND [NO] CHAIN` and `RELEASE` clauses. There is a new `RELEASE SAVEPOINT` statement. The `completion_type` system variable was added for setting the global and session default completion type.
- Security improvement: The server creates `.frm`, `.MYD`, `.MYI`, `.MRG`, `.ISD`, and `.ISM` table files only if a file with the same name does not already exist. Thanks to Stefano Di Paola <stefano.dipaola@wisec.it> for finding and informing us about this issue. (CVE-2005-0711)
- Added the `engine_condition_pushdown` system variable. For NDB, setting this variable to 1 permits processing of some `WHERE` clause conditions to be processed in NDB nodes before rows are sent to the MySQL server, rather than having rows sent to the server for evaluation.
- Support for the `ISAM` storage engine has been removed. If you have `ISAM` tables, you should convert them before upgrading. See [Changes Affecting Upgrades to 5.0](#).
- Added the `CREATE ROUTINE` and `ALTER ROUTINE` privileges, and made the `EXECUTE` privilege operational.
- `BIT` in column definitions now is a distinct data type; it no longer is treated as a synonym for `TINYINT(1)`.
- Added `cp932` (SJIS for Windows Japanese) and `euc_jpms` (UJIS for Windows Japanese) character sets.
- `MEMORY (HEAP)` can have `VARCHAR` fields.
- `SHOW DATABASES`, `SHOW TABLES`, `SHOW COLUMNS`, and so forth, display information about the `INFORMATION_SCHEMA` database. Also, several `SHOW` statements now accept a `WHERE` clause specifying which output rows to display. See [INFORMATION_SCHEMA Tables](#).
- `SHOW COLUMNS` now displays `NO` rather than blank in the `Null` output column if the corresponding table column cannot be `NULL`.
- When the `MyISAM` storage engine detects corruption of a `MyISAM` table, a message describing the problem now is written to the error log.
- A `VARCHAR` column can now contain up to 65535 bytes. In addition, `VARCHAR` columns now remember trailing spaces. For more details, see [The CHAR and VARCHAR Types](#).

**Note**

If the table handler does not support the new `VARCHAR` type, then it is converted to a `CHAR` column. Currently this happens for `NDB` tables.

- Added `--innodb-checksums` and `--innodb-doublewrite` options for `mysqld`.
- Added several `InnoDB` status variables. See [Server Status Variables](#).
- Added account-specific `MAX_USER_CONNECTIONS` limit, which enables you to specify the maximum number of concurrent connections for the account. Also, all limited resources now are counted per

account (instead of being counted per user + host pair as it was before). Use the `--old-style-user-limits` option to get the old behavior.

- Implemented support for XA transactions. See [XA Transactions](#). The implementation makes the `--innodb-safe-binlog` option obsolete, so it has been removed.
- `mysqlbinlog` now prints a `ROLLBACK` statement at the end of its output, in case the server crashed while it was in the process of writing the final entry into the last binary log named on the command line. This causes any half-written transaction to be rolled back when the output is executed. The `ROLLBACK` is harmless if the binary log file was written and closed normally.
- `Seconds_Behind_Master` is `NULL` (which means “unknown”) if the slave SQL thread is not running, or if the slave I/O thread is not running or not connected to master. It is zero if the SQL thread has caught up to the I/O thread. It no longer grows indefinitely if the master is idle.
- `FLUSH TABLES WITH READ LOCK` is now killable while it is waiting for running `COMMIT` statements to finish.
- The MySQL server aborts immediately instead of simply issuing a warning if it is started with the `--log-bin` option but cannot initialize the binary log at startup (that is, an error occurs when writing to the binary log file or binary log index file).
- The binary log file and binary log index file now are handled the same way as `MyISAM` tables when there is a “disk full” or “quota exceeded” error. See [How MySQL Handles a Full Disk](#).
- **InnoDB:** When MySQL/InnoDB is compiled on Mac OS X 10.2 or earlier, detect the operating system version at run time and use the `fctl()` file flush method on Mac OS X versions 10.3 and later. In Mac OS X, `fsync()` does not flush the write cache in the disk drive, but the special `fctl()` does; however, the flush request is ignored by some external devices. Failure to flush the buffers may cause severe database corruption at power outages.

Bugs Fixed

- **Replication:** If multiple semicolon-separated statements were received in a single packet, they were written to the binary log as a single event rather than as separate per-statement events. For a server serving as a replication master, this caused replication to fail when the event was sent to slave servers. (Bug #8436)
- **Replication:** A replication master stamped a generated statement (such as a `SET` statement) with an error code intended only for another statement. This could happen, for example, when a statement generated a duplicate key error on the master but still had to be replicated to the slave. (Bug #8412)
- **Replication:** If the slave was running with `--replicate-*-table` options which excluded one temporary table and included another, and the two tables were used in a single `DROP TEMPORARY TABLE IF EXISTS` statement, as the ones the master automatically writes to its binary log upon client's disconnection when client has not explicitly dropped these, the slave could forget to delete the included replicated temporary table. Only the slave needs to be upgraded. (Bug #8055)
- **Replication:** Multiple-table updates did not replicate properly to slave servers where `--replicate-*-table` options had been specified. (Bug #7011)
- **Replication:** A replication slave could crash after replicating many `ANALYZE TABLE`, `OPTIMIZE TABLE`, or `REPAIR TABLE` statements from the master. (Bug #6461, Bug #7658)
- **Replication:** Changed semantics of `CREATE/ALTER/DROP DATABASE` statements so that replication of `CREATE DATABASE` is possible when using `--binlog-do-db` and `--binlog-ignore-db`. (Bug #6391)

- **Replication:** DDL statements for views were not being written to the binary log (and thus not subject to replication). (Bug #4838)
- `mysqldump` misinterpreted “_” and “%” characters in the names of tables to be dumped as wildcard characters. (Bug #9123)
- In strict or traditional SQL mode, too-long string values assigned to string columns (`CHAR`, `VARCHAR`, `BINARY`, `VARBINARY`, `TEXT`, or `BLOB`) were correctly truncated, but the server returned an `SQLSTATE` value of `01000` (should be `22001`). (Bug #9029, Bug #6999)
- The definition of the enumeration-valued `sql_mode` column of the `mysql.proc` table was missing some of the current permissible SQL modes, so stored routines would not necessarily execute with the SQL mode in effect at the time of routine definition. (Bug #8902)
- `TRUNCATE TABLE` did not work within stored procedures. Now, within stored procedures, `TRUNCATE TABLE` is executed in the same way as `DELETE`. This change was necessary because `TRUNCATE TABLE` implicitly locks tables. (Bug #8850)
- A rare race condition could cause `FLUSH TABLES WITH READ LOCK` to hang. (Bug #8682)
- `AES_DECRYPT(col_name, key)` could fail to return `NULL` for invalid values in `col_name`, if `col_name` was declared as `NOT NULL`. (Bug #8669)
- If `SELECT DISTINCT` named an index column multiple times in the select list, the server tried to access different key fields for each instance of the column, which could result in a crash. (Bug #8532)
- `MATCH ... AGAINST` in natural language mode could cause a server crash if the `FULLTEXT` index was not used in a join (that is, `EXPLAIN` did not show `fulltext` join mode) and the search query matched no rows in the table. (Bug #8522)
- `REPAIR TABLE` did not invalidate query results in the query cache that were generated from the table. (Bug #8480)
- `LOAD INDEX` statement now loads the index into memory. (Bug #8452)
- For a stored function that refers to a given table, invoking the function while selecting from the same table resulted in a server crash. (Bug #8405)
- Comparison of a `DECIMAL` column containing `NULL` to a subquery that produced `DECIMAL` values resulted in a server crash. (Bug #8397)
- `DELETE FROM tbl_name ... WHERE ... ORDER BY tbl_name.col_name` when the `ORDER BY` column was qualified with the table name caused the server to crash. (Bug #8392)
- Stored functions that used cursors could return incorrect results. (Bug #8386)
- The Cyrillic letters `И` (`I`) and `SHORT И` (`Ї`) were treated as being the same character by the `utf8_general_ci` collation. (Bug #8385)
- When performing boolean full-text searches on `utf8` columns, a double-quote character in the search string caused the server to crash. (Bug #8351)
- The `--set-character-set` option for `myisamchk` was changed to `--set-collation`. The value needed for specifying how to sort indexes is a collation name, not a character set name. (Bug #8349)
- Corruption of `MyISAM` table indexes could occur with `TRUNCATE TABLE` if the table had already been opened. For example, this was possible if the table had been opened implicitly by selecting from a

`MERGE` table that mapped to the `MyISAM` table. The server now issues an error message for `TRUNCATE TABLE` under these conditions. (Bug #8306)

- For a query with both `GROUP BY` and `COUNT(DISTINCT)` clauses and a `FROM` clause with a subquery, `NULL` was returned for any `VARCHAR` column selected by the subquery. (Bug #8218)
- Selecting from an `INFORMATION_SCHEMA` table combined with a subquery on an `INFORMATION_SCHEMA` table caused an error with the message `Table tbl_name is corrupted`. (Bug #8164)
- Matching of table names by `mysqlhotcopy` now accommodates `DBD:mysql` versions 2.9003 and up, which implement identifier quoting. (Bug #8136)
- Re-execution of prepared statements containing subqueries caused the server to crash. (Bug #8125)
- A problem with equality propagation optimization for prepared statements and stored procedures caused a server crash upon re-execution of the prepared statement or stored procedure. (Bug #8115, Bug #8849)

References: See also: Bug #51650.

- Selecting from a view defined as a join caused a server crash if the query cache was enabled. (Bug #8054)
- Results in the query cache generated from a view were not properly invalidated after `ALTER VIEW` or `DROP VIEW` on that view. (Bug #8050)
- Creating a table using a name containing a character that is illegal in `character_set_client` resulted in the character being stripped from the name and no error. The character now is considered an error. (Bug #8041)
- Certain correlated subqueries with forward references (referring to an alias defined later in the outer query) could crash the server. (Bug #8025)
- Corrected a problem with references to `DUAL` where statements such as `SELECT 1 AS a FROM DUAL` would succeed but statements such as `SELECT 1 AS a FROM DUAL LIMIT 1` failed. (Bug #8023)
- Comparing a nested row expression (such as `ROW(1, (2, 3))`) with a subquery caused the server to crash. (Bug #8022)
- The number of columns in a row comparison against a subquery was calculated incorrectly. (Bug #8020)
- `mysqldump` now avoids writing `SET NAMES` to the dump output if the server is older than version 4.1 and would not understand that statement. (Bug #7997)
- A deadlock could occur on an update followed by a `SELECT` on an `InnoDB` table without any explicit locks being taken. `InnoDB` now takes an exclusive lock when `INSERT ON DUPLICATE KEY UPDATE` is checking duplicate keys. (Bug #7975)
- A slave running MySQL 3.23.51 or newer hung while trying to connect to a master running MySQL 3.23.50 or older. (This occurred due to a bug in the old masters—`SELECT @@unknown_var` caused the server to hang—which was fixed in MySQL 3.23.50.) (Bug #7965)
- Erroneous output resulted from `SELECT DISTINCT` combined with a subquery and `GROUP BY`. (Bug #7946)
- `FOUND_ROWS()` returned an incorrect value after a `SELECT SQL_CALC_FOUND_ROWS DISTINCT` statement that selected constants and included `GROUP BY` and `LIMIT` clauses. (Bug #7945)

- `mysqld_safe` now understands the `--help` option. Previously, it ignored the option and attempted to start the server anyway. (Bug #7931)
- Creating a user with grants failed when specifying a password but worked without one. (Bug #7905)
- Comparing the result of a subquery to a nonexistent column caused the server to crash. This issue affected MySQL on Windows platforms only. (Bug #7885)
- `ALTER TABLE` improperly accepted an index on a `TIMESTAMP` column that `CREATE TABLE` would reject. (Bug #7884)
- MySQL permitted concurrent updates (including inserts and deletes) to a table if binary logging was enabled. Now, all updates are executed in a serialized fashion, because they are executed serialized when the binary log is replayed. (Bug #7879)
- Ensured that `mysqldump --single-transaction` sets its transaction isolation level to `REPEATABLE READ` before proceeding (otherwise if the MySQL server was configured to run with a default isolation level lower than `REPEATABLE READ` it could give an inconsistent dump). (Bug #7850)
- `mysqlbinlog` forgot to add backquotes around the collation of user variables (causing later parsing problems as `BINARY` is a reserved word). (Bug #7793)
- A `Table is full` error occurred when the table was still smaller than `max_heap_table_size`. (Bug #7791)
- Use of `GROUP_CONCAT()` with `HAVING` caused the server to crash. (Bug #7769)
- The `CONV()` function returned an unsigned `BIGINT` number, which does not fit in 32 bits. (Bug #7751)
- The `IN()` operator did not return correct results if all values in the list were constants and some of them used substring functions such as `LEFT()`, `RIGHT()`, or `MID()`. (Bug #7716)
- When encountering a `disk full` or `quota exceeded` write error, `MyISAM` sometimes failed to sleep and retry the write, resulting in a corrupted table. (Bug #7714)
- The `CONVERT_TZ()` function, when its second or third argument was from a `const` table, caused the server to crash. (See [EXPLAIN Syntax](#).) (Bug #7705)
- The output of the `STATUS (\s)` command in `mysql` had the values for the server and client character sets reversed. (Bug #7571)
- A `LEFT OUTER JOIN` between an empty base table and a view on an empty base table caused a server crash. (Bug #7433)
- Ordering by an unsigned expression (more complex than a column reference) was treating the value as signed, producing incorrectly sorted results. `HAVING` was also treating unsigned columns as signed. (Bug #7425)
- The server crashed when an error occurred during the filling of a temporary table created for handling a view or derived table. (Bug #7413)
- Made the MySQL server accept executing `SHOW CREATE DATABASE` even if the connection has an open transaction or locked tables. Refusing it made `mysqldump --single-transaction` sometimes fail to print a complete `CREATE DATABASE` statement for some dumped databases. (Bug #7358)
- Handling of trailing spaces was incorrect for the `ucs2` character set. (Bug #7350)
- `--expire-logs-days` was not honored if using only transactions. (Bug #7236)

- Some `INFORMATION_SCHEMA` columns that contained timestamp values were of type `VARBINARY`. These were changed to `TIMESTAMP`. (Bug #7217)
- Some `INFORMATION_SCHEMA` columns that contained catalog identifiers were of type `LONGTEXT`. These were changed to `VARCHAR(N)`, where `N` is the appropriate maximum identifier length. (Bug #7215)
- Use of `GROUP_CONCAT()` in the select list when selecting from a view caused a server crash. (Bug #7116)
- An expression that tested a case-insensitive character column against string constants that differed in lettercase could fail because the constants were treated as having a binary collation. (For example, `WHERE city='London' AND city='london'` could fail.) (Bug #7098, Bug #8690)
- Setting the initial `AUTO_INCREMENT` value for an InnoDB table using `CREATE TABLE ... AUTO_INCREMENT = n` did not work, and `ALTER TABLE ... AUTO_INCREMENT = n` did not reset the current value. (Bug #7061)
- When setting integer system variables to a negative value with `SET VARIABLES`, the value was treated as a positive value modulo 2^{32} . (Bug #6958)
- Use of a view in a correlated subquery that contains `HAVING` but no `GROUP BY` caused a server crash. (Bug #6894)
- Preparing a query using the `CONVERT_TZ()` function with constant arguments caused the server to crash. (Bug #6849)
- Handling by `mysql_list_fields()` of references to stored functions within views was incorrect and could result in a server crash. (Bug #6814)
- A sequence of `BEGIN` (or `SET autocommit = 0`), `FLUSH TABLES WITH READ LOCK`, transactional update, `COMMIT`, `FLUSH TABLES WITH READ LOCK` could hang the connection forever and possibly the MySQL server itself. This happened for example when running the `innobackup` script several times. (Bug #6732)
- Prevent adding `CREATE TABLE .. SELECT` query to the binary log when the insertion of new records partially failed. (Bug #6682)
- `mysqlbinlog` did not print `SET PSEUDO_THREAD_ID` statements in front of `LOAD DATA INFILE` statements inserting into temporary tables, thus causing potential problems when rolling forward these statements after restoring a backup. (Bug #6671)
- If a `MyISAM` table on Windows had `INDEX DIRECTORY` or `DATA DIRECTORY` table options, `mysqldump` dumped the directory path names with single-backslash path name separators. This would cause syntax errors when importing the dump file. `mysqldump` now changes “\” to “/” in the path names on Windows. (Bug #6660)
- `SHOW CREATE TABLE` now reports `ENGINE=MEMORY` rather than `ENGINE=HEAP` for a `MEMORY` table (unless the `MYSQL323` SQL mode is enabled). (Bug #6659)
- Incorrectly ordered results were returned from a query using a `FULLTEXT` index to retrieve rows and there was another index that was usable for `ORDER BY`. For such a query, `EXPLAIN` showed the `fulltext` join type, but showed the other (not `FULLTEXT`) index in the `Key` column. (Bug #6635)
- `CREATE TABLE ... LIKE` failed on Windows when the source or destination table was located in a symlinked database directory. (Bug #6607)
- Retrieving from a view defined as a `SELECT` that mixed `UNION ALL` and `UNION DISTINCT` resulted in a different result than retrieving from the original `SELECT`. (Bug #6565)

- Selecting from a view that had an `EXISTS` or `NOT EXISTS` subquery did not always work properly, and selecting columns by name could cause a server crash. With `SELECT *`, crashes did not occur, but columns in the outer query were not resolved properly. (Bug #6394)
- Fixed a problem in `NO_BACKSLASH_ESCAPES` SQL mode for strings that contained both the string quoting character and backslash. (Bug #6368)
- The `CHAR()` function was not ignoring `NULL` arguments, contrary to the documentation. (Bug #6317)
- Starting and stopping the slave thread (only) could in some circumstance cause the server to crash. (Bug #6148)
- `InnoDB`: Honor the `--tmpdir` startup option when creating temporary files. Previously, `InnoDB` temporary files were always created in the temporary directory of the operating system. On Netware, `InnoDB` will continue to ignore `--tmpdir`. (Bug #5822)
- A `HAVING` clause that referred to `RAND()` or a user-defined function in the `SELECT` part of a query through an alias could cause MySQL to crash or to return an incorrect value. (Bug #5185)
- `mysql_fix_privilege_tables` now makes it possible for `mysql` privilege tables created in MySQL 5.0 to be used with MySQL 4.1. This makes it possible to downgrade from 5.0 to 4.1, or to run MySQL 4.1 and 5.0 using the same privilege table files for testing purposes.
- Giving `mysqld` a `SIGHUP` caused it to crash.
- Platform and architecture information in version information produced for `--version` option on Windows was always `Win95/Win98 (i32)`. More accurately determine platform as `Win32` or `Win64` for 32-bit or 64-bit Windows, and architecture as `ia32` for x86, `ia64` for Itanium, and `axp` for Alpha. (Bug #4445)
- When using the `RPAD()` function (or any function adding spaces to the right) in a query that had to be resolved by using a temporary table, all resulting strings had rightmost spaces removed (that is, `RPAD()` did not work) (Bug #4048)
- Prepared statements using `SUM(DISTINCT...)` did not perform correctly.
- `InnoDB`: Use native `tmpfile()` function on Netware. All `InnoDB` temporary files are created under `sys:\tmp`. Previously, `InnoDB` temporary files were never deleted on Netware.
- A symlink vulnerability in the `mysqlaccess` script was reported by Javier Fernandez-Sanguino Pena and [Debian Security Audit Team](#). (CVE-2005-0004)
- Host name matching didn't work if a netmask was specified for table-specific privileges. (Bug #3309)
- A number of portability issues relating to overflow in floating point values were corrected.
- Prepared statements now gives warnings on prepare.
- The combination of `-not` and `trunc*` operators in a full-text search did not work correctly. Using more than one truncated negative search term caused the result to be empty.
- Prepared statements did not work correctly with `OUTER JOIN`.

Changes in MySQL 5.0.2 (2004-12-01)

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- **Incompatible Change:** The precedence of `NOT` operator has changed so that expressions such as `NOT a BETWEEN b AND c` are parsed correctly as `NOT (a BETWEEN b AND c)` rather than as `(NOT a) BETWEEN b AND c`. The pre-5.0 higher-precedence behavior can be obtained by enabling the new `HIGH_NOT_PRECEDENCE` SQL mode.
- **Incompatible Change:** `SHOW STATUS` now shows the session (thread-specific) status variables and `SHOW GLOBAL STATUS` shows the status variables for the whole server.

Before MySQL 5.0.2, `SHOW STATUS` returned global status values. Because the default as of 5.0.2 is to return session values, this is incompatible with previous versions. To issue a `SHOW STATUS` statement that will retrieve global status values for all versions of MySQL, write it like this:

```
SHOW /*!50002 GLOBAL */ STATUS;
```

- **Replication:** `mysqldump --single-transaction --master-data` is now able to take an online (nonblocking) dump of `InnoDB` and report the corresponding binary log coordinates, which makes a backup suitable for point-in-time recovery, roll-forward or replication slave creation. See [mysqldump — A Database Backup Program](#).
- **Replication:** Two new system variables were introduced. `auto_increment_increment` and `auto_increment_offset` can be set locally or globally, and are intended for use in controlling the behavior of `AUTO_INCREMENT` columns in master-to-master replication. Note that these variables are not intended to take the place of sequences. See [Server System Variables](#).
- If the server finds that the `user` table has not been upgraded to include the view-related privilege columns, it treats each account as having view privileges that are the same as its `CREATE` privilege.
- A connection doing a rollback now displays "Rolling back" in the `State` column of `SHOW PROCESSLIST`.
- Renamed the `sql_updatable_view_key` system variable to `updatable_views_with_limit`. This variable now can have only two values:
 - `1` or `YES`: Don't issue an error message (warning only) if a `VIEW` without presence of a key in the underlying table is used in queries with a `LIMIT` clause for updating. (This is the default value.)
 - `0` or `NO`: Prohibit update of a `VIEW`, which does not contain a key in the underlying table and the query uses a `LIMIT` clause (usually get from GUI tools).
- Reverted output format of `SHOW TABLES` to old pre-5.0.1 format that did not include a table type column. To get the additional column that lists the table type, use `SHOW FULL TABLES` now.
- `CHECK TABLE` now works for views.
- Modify `DROP USER` so that it drops the account, including all its privileges. Formerly, it removed the account record only for an account that had all privileges revoked.
- `0` or `NO`: Prohibit update of a `VIEW`, which does not contain a key in the underlying table and the query uses a `LIMIT` clause (usually get from GUI tools).
- We now detect too-large floating point numbers during statement parsing and generate an error messages for them.
- If a write to a `MyISAM` table fails because of a full disk or an exceeded disk quota, it now prints a message to the error log every 10 minutes, and waits until disk space becomes available. (Bug #3248)
- New `auto_increment_increment` and `auto_increment_offset` system variables. These enable you to set up a server to generate auto-increment values that don't conflict with another server.

- Added the `CREATE USER` and `RENAME USER` statements.
- MySQL now by default checks dates and in strict mode permits only fully correct dates. If you want MySQL to behave as before, you should enable the new `ALLOW_INVALID_DATES` SQL mode.
- Added `NO_AUTO_CREATE_USER` SQL mode to prevent `GRANT` from automatically creating new users if it would otherwise do so, unless a password also is specified.
- Made the MySQL server ignore `SIGHUP` and `SIGQUIT` on Mac OS X 10.3. This is needed because under this OS, the MySQL server receives lots of these signals. (Bug #2030)
- MySQL now remembers which columns were declared to have default values. In `STRICT_TRANS_TABLES/STRICT_ALL_TABLES` mode, you now get an error if you do an `INSERT` without specifying all columns that don't have a default value. A side effect of this is that when you do `SHOW CREATE` for a new table, you no longer see a `DEFAULT` value for a column for which you didn't specify a default value.
- **InnoDB:** If you specify the `innodb_locks_unsafe_for_binlog` option in `my.cnf`, for an `UPDATE` or a `DELETE`, InnoDB locks only the rows that it updates or deletes. This greatly reduces the probability of deadlocks.
- A `HAVING` clause in a `SELECT` statement now can refer to columns in the `GROUP BY` clause, as required by standard SQL.
- The `SCHEMA` and `SCHEMAS` keywords are now accepted as synonyms for `DATABASE` and `DATABASES`.
- Added several InnoDB status variables. See [Server Status Variables](#).
- Added `STRICT_TRANS_TABLES`, `STRICT_ALL_TABLES`, `NO_ZERO_IN_DATE`, `NO_ZERO_DATE`, `ERROR_FOR_DIVISION_BY_ZERO`, and `TRADITIONAL` SQL modes. The `TRADITIONAL` mode is shorthand for all the preceding modes. When using mode `TRADITIONAL`, MySQL generates an error if you try to insert a wrong value in a column. It does not adjust the value to the closest possible legal value.
- The `mysql_fix_privilege_tables` script now initializes the global `CREATE VIEW` and `SHOW VIEW` privileges in the `user` table to the value of the `CREATE` privilege in that table.
- `1` or `YES`: Don't issue an error message (warning only) if a VIEW without presence of a key in the underlying table is used in queries with a `LIMIT` clause for updating. (This is the default value.)
- The compilation flag `DONT_USE_DEFAULT_FIELDS` was removed because you can get the same behavior by setting the `sql_mode` system variable to `STRICT_TRANS_TABLES`.
- `mysqlbinlog` now prints an informative commented line (thread id, timestamp, server id, and so forth) before each `LOAD DATA INFILE`, like it does for other queries; unless `--short-form` is used.
- Added `IS [NOT] boolean_value` syntax, where `boolean_value` is `TRUE`, `FALSE`, or `UNKNOWN`.
- Added `--start-datetime`, `--stop-datetime`, `--start-position`, and `--stop-position` options to `mysqlbinlog`. These make point-in-time recovery easier.
- Added initial support for rudimentary triggers (the `CREATE TRIGGER` and `DROP TRIGGER` statements).
- Added basic support for read-only server side cursors.
- Implemented the `WITH CHECK OPTION` clause for `CREATE VIEW`.
- Added support for the `INFORMATION_SCHEMA` "information database" that provides database metadata. See [INFORMATION_SCHEMA Tables](#).

Bugs Fixed

- **Replication:** A problem introduced in MySQL 4.0.21 caused replication slaves to stop (error 1223) where a connection started a transaction, performed updates, then issued a `FLUSH TABLES WITH READ LOCK` followed by a `COMMIT`. This issue occurred when using the InnoDB `innobackup` script. (Bug #5949)
- **Replication:** `SET COLLATION_SERVER...` statements replicated by the slave SQL thread no longer advance its position. This is so that, if the thread is interrupted before the update is completed, it later performs the `SET` again. (Bug #5705)
- **Replication:** `OPTIMIZE TABLE`, `REPAIR TABLE`, and `ANALYZE TABLE` are now replicated without any error code in the binary log. (Bug #5551)
- **Replication:** A `CREATE TABLE ... TYPE=HEAP ... AS SELECT...` statement caused the replication slave to stop. (Bug #4971)
- `mysqlbinlog` was unable to read from `stdin`, for example, when piping the output from `zcat` to `mysqlbinlog`. (Bug #7853)
- If a connection was interrupted by a network error and did a rollback, the network error code got stored into the `BEGIN` and `ROLLBACK` binary log events; that caused superfluous slave stops. (Bug #6522)
- If a connection had an open transaction but had done no updates to transactional tables (for example if had just done a `SELECT FOR UPDATE` then executed a nontransactional update, that update automatically committed the transaction (thus releasing InnoDB's row-level locks etc). (Bug #5714)
- If the slave SQL thread finds a syntax error in a query (which should be rare, as the master parsed it successfully), it now stops immediately. (Bug #5711)
- `disable-local-infile` option had no effect if the client read it from a configuration file using `mysql_options(...,MYSQL_READ_DEFAULT,...)`. (Bug #5073)
- `SET GLOBAL SYNC_BINLOG` did not work on some platforms (Mac OS X). (Bug #5064)
- `mysql-test-run` failed the `rpl_trunc_binlog` test when running the test from the installation directory. (Bug #5050)
- `mysql_options(...,MYSQL_OPT_LOCAL_INFILE,...)` failed to disable `LOAD DATA LOCAL INFILE`. (Bug #5038)
- The counter for an `AUTO_INCREMENT` column was not reset by `TRUNCATE TABLE` if the table was a temporary one. (Bug #5033)
- `FLUSH TABLES WITH READ LOCK` now blocks `COMMIT` statements if the server is running with binary logging enabled; this ensures that the binary log position is trustable when doing a full backup of tables and the binary log. (Bug #4953)
- `KILL`ing a connection while it was performing `START SLAVE` caused the server to crash. (Bug #4827)
- A deadlock could happen under certain rare circumstances when using `KILL`. (Bug #4810)
- `mysql-test-run` failed the `grant_cache` test when run as Unix root user. (Bug #4678)
- `mysqlbinlog --read-from-remote-server` sometimes could not accept 2 binary logs in a single invocation. (Bug #4507)
- `mysqlbinlog --position --read-from-remote-server` had incorrect output for `# at log_pos`. (Bug #4506)

Changes in MySQL 5.0.1 (2004-07-27)



Note

This build passes our test suite and fixes a lot of reported bugs found in the previous 5.0.0 release. However, please be aware that this is not a “standard MySQL build” in the sense that there are still some open critical bugs in our bugs database at <http://bugs.mysql.com/> that affect this release as well. We are actively fixing these and will make a new release where these are fixed as soon as possible. However, this binary should be a good candidate for testing new MySQL 5.0 features for future products.

- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

Functionality Added or Changed

- **Incompatible Change:** C API change: `mysql_shutdown()` now requires a second argument. This is a source-level incompatibility that affects how you compile client programs; it does not affect the ability of compiled clients to communicate with older servers. See [mysql_shutdown\(\)](#).
- **Replication:** Added the `--replicate-same-server-id` server option.
- **Replication:** For replication of `MEMORY (HEAP)` tables: Made the master automatically write a `DELETE FROM` statement to its binary log when a `MEMORY` table is opened for the first time since the master's startup. This is for the case where the slave has replicated a nonempty `MEMORY` table, and then the master is shut down and restarted: the table is now empty on the master; the `DELETE FROM` empties it on the slave as well.

Even with this fix, between the master's restart and the first use of the table on master, the slave still has out-of-date data in the table. However, if you use the `--init-file` option to populate the `MEMORY` table on the master at startup, it ensures that the failing time interval is zero. (Bug #2477)

- **Replication:** `DROP DATABASE IF EXISTS`, `DROP TABLE IF EXISTS`, single-table `DELETE`, and single-table `UPDATE` now are written to the binary log even if they changed nothing on the master (for example, even if a `DELETE` matched no rows). The old behavior sometimes caused bad surprises in replication setups.
- **Replication:** Replication and `mysqlbinlog` now have better support for the case that the session character set and collation variables are changed within a given session. See [Replication Features and Issues](#).
- The `Type` column name and values in the output from `SHOW TABLES` are now shown according to standard. The column name has changed from `Type` to `table_type`; permitted values are `BASE TABLE`, `VIEW`, and `ERROR`. (Bug #4603)
- Added `Last_query_cost` status variable that reports optimizer cost for last compiled query.
- Changed that when the MySQL server has binary logging disabled (that is, no `--log-bin` option was used), then no transaction binary log cache is allocated for connections. This should save `binlog_cache_size` bytes of memory (32KB by default) for every connection.
- Implemented a new “greedy search” optimizer that can significantly reduce the time spent on query optimization for some many-table joins. (You are affected if not only some particular `SELECT` is slow, but even using `EXPLAIN` for it takes a noticeable amount of time.) Two new system variables,

`optimizer_search_depth` and `optimizer_prune_level`, can be used to fine-tune optimizer behavior.

- `OPTIMIZE TABLE` for InnoDB tables is now mapped to `ALTER TABLE` instead of `ANALYZE TABLE`. This rebuilds the table, which updates index statistics and frees space in the clustered index.
- When a session having open temporary tables terminates, the statement automatically written to the binary log is now `DROP TEMPORARY TABLE IF EXISTS` instead of `DROP TEMPORARY TABLE`, for more robustness.
- Added support for read-only and updatable views based on a single table or other updatable views. View use requires that you upgrade your grant tables to add the view-related privileges. See [mysql_fix_privilege_tables — Upgrade MySQL System Tables](#).
- Added the `sql_updatable_view_key` system variable.
- The MySQL server now returns an error if `SET sql_log_bin` is issued by a user without the `SUPER` privilege (in previous versions it just silently ignored the statement in this case).
- When a database is dropped, all routines belonging to that database are also dropped.
- Added the `--to-last-log` option to `mysqlbinlog`, for use in conjunction with `--read-from-remote-server`.
- `sync_frm` is now a settable global variable (not only a startup option).
- Added `--innodb-safe-binlog` server option, which adds consistency guarantees between the content of InnoDB tables and the binary log. See [The Binary Log](#).
- Explicit `USE db_name` statements no longer are permitted in a stored procedure.
- Added the `sync_binlog=N` global variable and startup option, which makes the MySQL server synchronize its binary log to disk (`fdatasync()`) after every Nth write to the binary log.
- Killing a `CHECK TABLE` statement does not result in the table being marked as “corrupted” any more; the table remains as if `CHECK TABLE` had not even started. See [KILL Syntax](#).
- Changed the slave SQL thread to print less useless error messages (no more message duplication; no more messages when an error is skipped because of `slave-skip-errors`).
- When executed from another database, an implicit `USE db_name` is in effect.
- When installing a MySQL server as a Windows service, the installation command can include a `--local-service` option following the service name to cause the server to run using the `LocalService` Windows account that has limited privileges. This is in addition to the `--defaults-file` option that also can be given following the service name.
- Procedure names may be qualified, for example, `db.p()`
- A stored procedure is no longer “global.” That is, it now belongs to a specific database:
 - When a database is dropped, all routines belonging to that database are also dropped.
 - Procedure names may be qualified, for example, `db.p()`
 - When executed from another database, an implicit `USE db_name` is in effect.
 - Explicit `USE db_name` statements no longer are permitted in a stored procedure.

See [Using Stored Routines \(Procedures and Functions\)](#).

Bugs Fixed

- **Replication:** When a multiple-table `DROP TABLE` failed to drop a table on the master server, the error was not written to the binary log. (Bug #4553)
- **Replication:** When the slave SQL thread was replicating a `LOAD DATA INFILE` statement, it didn't show the statement in the output of `SHOW PROCESSLIST`. (Bug #4326)
- **Replication:** Complex expressions using `AND`, `OR`, or both could result in a crash if the query containing the expression query was ignored, either by a replication server due to `--replicate-*-table` rules, or by any MySQL server due to a syntax error. (Bug #3969, Bug #4494)
- **Replication:** The slave SQL thread refused to replicate `INSERT ... SELECT` if it examined more than 4 billion rows. (Bug #3871)
- **Replication:** If `server-id` was not set using startup options but with `SET GLOBAL`, the replication slave still complained that it was not set. (Bug #3829)
- **Replication:** A MySQL slave server built using `--with-debug`, and replicating itself, crashed. (Bug #3568)
- **Replication:** Multiple-table `DELETE` statements were always replicated by the slave if there were some `--replicate-*-ignore-table` options and no `--replicate-*-do-table` options. (Bug #3461)
- **Replication:** Memory could be corrupted by replicating a `LOAD DATA INFILE` from a MySQL 3.23 master. Some less critical issues remain; see [Replication Features and Issues](#). (Bug #3422)
- **Replication:** In some replication error messages, a very long query caused the rest of the message to be invisible (truncated), by putting the query last in the message. (Bug #3357)
- **Replication:** Changed that when a thread handling `INSERT DELAYED` (also known as a `delayed_insert` thread) is killed, its statements are recorded with an error code of value zero (killing such a thread does not endanger replication, so we thus avoid a superfluous error on the slave). (Bug #3081)
- **Replication:** Corrected the master's binary log position that `InnoDB` reports when it is doing a crash recovery on a slave server. (Bug #3015)
- **Replication:** `--replicate-wild-*-table` rules now apply to `ALTER DATABASE` when the table pattern is `%`, as is the case for `CREATE DATABASE` and `DROP DATABASE`. (Bug #3000)
- **Replication:** Statements did not raise errors on the slave, if the slave was excluded given the `--replicate-*` options in use at the time. The effect of this problem was: when a statement was killed on the master, the slave stopped. (Bug #2983)
- **Replication:** Multiple-table `DELETE` statements were never replicated by the slave if there were any `--replicate-*-table` options. (Bug #2527)
- **Replication:** Replication: If a client connects to a slave server and issues an administrative statement for a table (for example, `OPTIMIZE TABLE` or `REPAIR TABLE`), this could sometimes stop the slave SQL thread. This does not lead to any corruption, but you must use `START SLAVE` to get replication going again. (Bug #1858)
- If `CREATE TEMPORARY TABLE t SELECT` failed while loading the data, the temporary table was not dropped. (Bug #4551)

- `mysql_fix_privilege_tables` did not handle the `--password=password_val` option correctly. (Bug #4240, Bug #4543)
- Made `DROP DATABASE` honor the value of `lower_case_table_names`. (Bug #4066)
- During the installation process of the server RPM on Linux, if `mysqld` was run as the `root` system user and with `--log-bin` pointing to a directory outside of `/var/lib/mysql`, it created binary log files owned by `root` in this directory, which remained owned by `root` after the installation. Now `mysqld` is started as the `mysql` system user instead. (Bug #4038)
- A potential memory overrun could occur in `mysql_real_connect()` (which required a compromised DNS server and certain operating systems). (Bug #4017)
- `mysqlbinlog` didn't escape the string content of user variables, and did not deal well when these variables were in non-ASCII character sets; this is now fixed by always printing the string content of user variables in hexadecimal. The character set and collation of the string is now also printed. (Bug #3875)
- `mysqlbinlog` failed to print a `USE` statement under those rare circumstances where the binary log contained a `LOAD DATA INFILE` statement. (Bug #3415)
- A rare error condition caused the slave SQL thread spuriously to print the message `Binlog has bad magic number` and stop when it was not necessary to do so. (Bug #3401)
- `mysqlbinlog --read-from-remote-server` now print the exact positions of events in lines beginning with `at #` in the log. (Bug #3214)
- `mysqlbinlog --read-from-remote-server` read all binary logs following the one that was requested. It now stops at the end of the requested file, the same as it does when reading a local binary log. There is an option `--to-last-log` to get the old behavior. (Bug #3204)
- Strange results with index (x, y) ... `WHERE x=val_1 AND y>=val_2 ORDER BY pk`; (Bug #3155)
- Adding `ORDER BY` to a query that uses a subquery can cause incorrect results. (Bug #3118)
- Changed that when a `DROP TEMPORARY TABLE` statement is automatically written to the binary log when a session ends, the statement is recorded with an error code of value zero (this ensures that killing a `SELECT` on the master does not result in a superfluous error on the slave). (Bug #3063)
- When a `Rotate` event was found by the slave SQL thread in the middle of a transaction, the value of `Relay_Log_Pos` in `SHOW SLAVE STATUS` was incorrectly altered. (Bug #3017)
- Running `LOAD DATA FROM MASTER` after `RESET SLAVE` caused a segmentation fault. (Bug #2922)
- A deadlock occurred when two `START SLAVE` statements were run at the same time. (Bug #2921)
- Changed the column `Seconds_Behind_Master` in `SHOW SLAVE STATUS` to never show a value of -1. (Bug #2826)
- Made clearer the error message that one gets when an update is refused because of the `--read-only` option. (Bug #2757)
- The MySQL server did not report any error if a statement (submitted through `mysql_real_query()` or `mysql_stmt_prepare()`) was terminated by garbage characters. This can happen if you pass a wrong `length` parameter to these functions. The result was that the garbage characters were written into the binary log. (Bug #2703)
- `SLAVE START` (which is a deprecated syntax, `START SLAVE` should be used instead) could crash the slave. (Bug #2516)

- The `--local-load` option of `mysqlbinlog` now requires an argument.
- `ALTER DATABASE` caused the client to hang if the database did not exist. (Bug #2333)

Changes in MySQL 5.0.0 (2003-12-22, Alpha)

Functionality Added or Changed

- **Important Change:** If you upgrade to MySQL 4.1.1 or higher, it is difficult to downgrade back to 4.0 or 4.1.0. That is because, for earlier versions, `InnoDB` is not aware of multiple tablespaces.
- **Replication:** Easier replication upgrade (5.0.0 masters can read older binary logs and 5.0.0 slaves can read older relay logs). See [Replication Compatibility Between MySQL Versions](#), for more details). The format of the binary log and relay log is changed compared to that of MySQL 4.1 and older.
- **Replication:** New binary log format that enables replication of these session variables: `sql_mode`, `sql_auto_is_null`, `foreign_key_checks` (which was replicated since 4.0.14, but here it is done more efficiently and takes less space in the binary logs), `unique_checks`. Other variables (like character sets, `sql_select_limit`, ...) will be replicated in upcoming 5.0.x releases.
- Added `TIMESTAMPADD()` and `TIMESTAMPDIFF()` functions.
- The `KILL` statement now takes `CONNECTION` and `QUERY` modifiers. The first is the same as `KILL` with no modifier (it kills a given connection thread). The second kills only the statement currently being executed by the connection.
- Added support for `SUM(DISTINCT)`, `MIN(DISTINCT)`, and `MAX(DISTINCT)`.
- Basic support for stored procedures and functions (SQL:2003 style). See [Using Stored Routines \(Procedures and Functions\)](#).
- The output of the `SHOW BINLOG EVENTS` statement has been modified. The `Orig_log_pos` column has been renamed to `End_log_pos` and now represents the offset of the last byte of the event, plus one.
- Implemented Index Merge optimization for `OR` clauses. See [Index Merge Optimization](#).
- For user-defined functions (UDFs), the `UDF_ARGS` structure now has `attributes` and `attribute_lengths` members that provide information about the argument names. [UDF Argument Processing](#).
- Added `WEEK` and `QUARTER` values as `INTERVAL` arguments for the `DATE_ADD()` and `DATE_SUB()` functions.
- The precedence of the `XOR` operator now lies between `OR` and `AND`. Previously, `XOR` had the same precedence as `OR`.
- Added `SELECT ... INTO list_of_vars`, which can be of mixed (that is, global and local) types. See [SELECT ... INTO Syntax](#).
- `LOAD DATA INFILE` causes an implicit commit.



Important

The behavior of `LOAD DATA INFILE` in this regard was changed again in MySQL 5.0.26. See [Changes in MySQL 5.0.26 \(2006-10-03\)](#).

