Oracle® Linux

UEFI Secure Boot Update Notices

F12070-06
October 2020

Oracle Legal Notices

Copyright © 2020, Oracle and/or its affiliates.

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 embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. 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 Inside 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, Epyc, and the AMD 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.

Abstract

This document contains information about updates to the UEFI Secure Boot signing keys used by Oracle to sign kernels and grub packages released by Oracle. Updates may affect users of both the Unbreakable Enterprise Kernel and Red Hat Compatible Kernel (RHCK) on systems that are configured for UEFI Secure Boot. This document may be updated after it is released. To check for updates to this document, and to view other Oracle documentation, refer to the Documentation section on the Oracle Technology Network (OTN) Web site:

https://docs.oracle.com/en/operating-systems/linux.html

This document is intended for users and administrators of Oracle Linux. It describes updates to the UEFI Secure Boot signing keys used by Oracle to sign kernels and grub packages released by Oracle. These updates affect users of both the Unbreakable Enterprise Kernel and Red Hat Compatible Kernel (RHCK) on systems that are configured for UEFI Secure Boot. The document provides instructions on how to update your system if you are using UEFI Secure Boot and how to handle a downgrade in the event that you need to use a kernel signed by an earlier signing key. Oracle recommends that you read this document before upgrading or downgrading your kernel if you use UEFI Secure Boot.

Document generated on: 2020-10-09 (revision: 10859)

Table of Contents

Preface

The *Oracle Linux UEFI Secure Boot Signing Key Update Notice* provides information about an update to The UEFI Secure Boot signing key used by Oracle to sign kernels and related packages that are used for UEFI Secure Boot.

Audience

This document is written for system administrators who want to use UEFI Secure Boot with Oracle Linux. It is assumed that readers have a general understanding of the Linux operating system.

Related Documents

The latest version of this document and other documentation for this product are available at:

https://docs.oracle.com/en/operating-systems/linux.html.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle recognizes the influence of ethnic and cultural values and is working to remove language from our products and documentation that might be considered insensitive. While doing so, we are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is an ongoing, long-term process.

Chapter 1 Notices

Table of Contents

A system in Secure Boot mode only loads boot loaders and kernels that have been signed by Oracle. Oracle updates the kernel and grub2 packages to sign them with a valid Extended Validation (EV) certificate in the event that a key may expire or for additional security updates. The EV certificate is compiled into the shim binary and is signed by Microsoft. This feature is fully supported from Oracle Linux 7 Update 3 onward.

All kernels and affected packages released previously should continue to work at their current version. However, if you intend to update kernel or packages, these notices apply and you should perform an atomic update in accordance with the instructions provided here.

The following sections describe events where the kernels and associated packages are updated with new keys. Each section describes the minimum kernel versions affected by the change and the package versions that are updated with the new keys.

1.1 [2020-07-29] Key update for CVE-2020-10713

Oracle has updated the key that it uses to sign UEK kernels and grub instances in response to CVE-2020-10713. This update affects users on Oracle Linux 7 and Oracle Linux 8.

Newer kernel versions are signed with the new key and require that other components are updated as an atomic operation if you upgrade the system .

Oracle Linux 7

On Oracle Linux 7 the following kernel package versions, or higher, are signed with the new key:

- **Red Hat Compatible Kernel (RHCK).** v3.10.0-1127.18.2
- **Unbreakable Enterprise Kernel Release 3 (UEK R3).** v3.8.13-118.47.2
- **Unbreakable Enterprise Kernel Release 4 (UEK R4).** v4.1.12-124.40.6.3
- **Unbreakable Enterprise Kernel Release 5 (UEK R5).** v4.14.35-1902.304.6.3
- **Unbreakable Enterprise Kernel Release 6 (UEK R6).** v5.4.17-2011.4.6

The following package versions are signed using the same EV certificate as the latest kernel releases:

- **`grub2`.** v2.02-0.82.0.5 (required)
- **`shim-x64`.** v15-2.0.5 (required)
- **`fwupdate-efi`.** v12-5.0.5 (optional)

Oracle Linux 8

On Oracle Linux 8 the following kernel package versions, or higher, are signed with the new key:

- **Red Hat Compatible Kernel (RHCK).** v4.18.0-193.14.3
- **Unbreakable Enterprise Kernel Release 6 (UEK R6).** v5.4.17-2011.4.6

The following package versions are signed using the same EV certificate as the latest kernel releases:

- **`grub2`.** v2.02-82.0.2 (required)
- **`shim-x64`.** v15-11.0.5 (required)
- **`fwupdate-efi`.** v11-3.0.3.el8 (optional)
- **`fwupd`.** v1.1.4-6.0.2.el8 (optional)

1.2 [2018-11-15] Key expiry update

Oracle has updated the key that it uses to sign kernels and grub instances to avoid key expiry. This update affects users on Oracle Linux 7.

Newer kernel versions are signed with the new key and require that other components are updated as an atomic operation if you upgrade the system .

The update affects all UEK releases, as well as the RHCK. The following kernel package versions, or higher, are signed with the new key:

- **Red Hat Compatible Kernel (RHCK).** v3.10.0-957.0
- **Oracle Modified Red Hat Compatible Kernel (RHCK).** v3.10.0-957.0.0.0.2
- **Unbreakable Enterprise Kernel Release 3 (UEK R3).** v3.8.13-118.27.1
- **Unbreakable Enterprise Kernel Release 4 (UEK R4).** v4.1.12-124.22.1
- **Unbreakable Enterprise Kernel Release 5 (UEK R5).** v4.14.35-1818.4.6

The following package versions are signed using the same EV certificate as the latest kernel releases:

- **`grub2`.** v2.02-0.76.0.3 (required)
- **`shim-x64`.** v15-1.0.3 (required)
- **`fwupdate-efi`.** v12-5.0.3 (optional)

Chapter 2 Action Items

Table of Contents

If you are using UEFI Secure Boot, you should be aware of the following action items when upgrading or downgrading packages on your system.

2.1 Upgrading

If you have previously enabled Secure Boot and you intend to upgrade your kernel, you must ensure that you update `shim-x64`, `grub2` and `kernel` packages as an atomic operation. If these packages are not all updated, the Secure Boot process may break and must be disabled until a full system upgrade is complete.

The `fwupdate-efi` package is also affected by this update. Although this package is not essential for boot, you may wish to update it to a version that is equal to or higher than the versions listed below if you have it installed.

If you upgrade your kernel to a version that is equal to, or higher than, a version signed with a new EV certificate, as described in Chapter 1, *Notices*, make sure the associated packages are upgraded to the specified versions or later.

You should pay attention to determine whether the kernel version that you intend to install or upgrade to is affected by a key update and install the appropriate minimum package versions at the same time.

2.2 Downgrading

If you have enabled Secure Boot, are running a current kernel version signed with the latest EV certificate, and you intend to downgrade kernel to a version lower than any listed in Chapter 1, *Notices*; you must downgrade the `shim-x64`, `grub2` and `kernel` packages as an atomic operation. Ensure that the `shim` and `grub2` packages are *lower* than the versions listed in Chapter 1, *Notices*.

You should pay attention to determine whether the kernel version that you intend to downgrade to is affected by an alternate key update and install the appropriate package versions at the same time.