Title: Improper initialization of Non-orderly TPM shut-down may result in susceptibility to dictionary attack vulnerability

ID: TCG-SA-2020-001

Released: Original: 2020-11-10 Last Revised: 2020-11-10

Related CVE ID's and associated CVSSv3 vector and score
CVE: CVE-2020-26933

CVSS base score: 7.2 High

CVSS Vector: CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N

CWE-665: Improper Initialization

Overview
A vulnerability was found in the reference code of Trusted Computing Group (TCG) Trusted Platform Module (TPM) 2.0 Library Specification Revisions 1.38 and 1.59 which could potentially impact the TPM implementation of non-orderly shutdown-failedTries with the USE_DA_USED build flag.

Description
The reference code does not correctly implement the behavior described in the aforementioned specifications if a DA protected object is accessed after a TPM2_Shutdown(). In this case, the NV flag (indicating that access to a DA protected object occurred during this boot cycle) is not set correctly. When a power loss happens, failedTries is not incremented on the next TPM2_Startup().

The check and increment of failedTries on TPM2_Startup() ensures that a failed authorization attempt is recorded by the TPM (e.g. because NV memory is unavailable).

Impact
Exploitation on vulnerable systems may result in local information disclosure or escalation of privileges.

Exposure of this issue is on TPM implementations where the NVM device may be measured or controlled by an attacker.

Solution and Protective Measures
Review and implement TCG publications: Errata 1.11 for revision 1.38 in section 2.36 and Errata 1.1 for revision 1.59 in section 2.2.

Acknowledgement

- The vulnerability was found by Intel Corporation

Vendor Information

- Vendor References

AMD:	CVE-2020-12926 https://www.amd.com/en/corporate/product-security
Intel:	CVE-2020-8744, https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00391.html