Title: TPM 2.0 Library Out-of-Bound Read Vulnerability

ID: TCGVRT0009

Released: 2025-JUN-10

CVE: CVE-2025-2884

CVSS Base Score: 6.6 Medium

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

Overview:

A vulnerability was found in the TPM 2.0 reference implementation code published by the Trusted Computing Group, Revisions 1.83, 1.59 and 1.38 which could potentially result in information disclosure or denial of service of the TPM.

The TPM 2.0 Library Specification (https://trustedcomputinggroup.org/resource/tpm-library-specification/) is prone to a potential out-of-bounds read vulnerability, as identified by a security researcher. The reported vulnerability occurs when inconsistent parameters are used in TPM 2.0 commands. The vulnerability is in the `CryptHmacSign` function, which is defined in the [Part 4: Supporting Routines – Code] (https://trustedcomputinggroup.org/wp-content/uploads/TPM-2.0-1.83-Part-4-Supporting-Routines-Code.pdf) document, section "7.151 - /tpm/src/crypt/CryptUtil.c ". The out-of-bounds read vulnerability is identified as CVE-2025-2884. This vulnerability can be triggered from user-mode applications by sending malicious commands to a TPM 2.0 whose firmware is based on an affected TCG reference implementation.

Description:

The reference code did not implement appropriate consistency check in CryptHmacSign() resulting in potential out-of-bound read. The out-of-bound read occurs on the buffer passed to the ExecuteCommand() entry point (detailed in Part 4 of the spec.) CVE-2025-2884 may allow an attacker to read up to 65535 bytes past the end of that buffer. Depending upon the size of the buffer the impact assessment may vary across various TPM implementations and vendors.

Impact:

Exploitation on vulnerable systems may result in information disclosure or denial of service of the TPM. The impact assessment depends on the vendor specific implementation.

Solution and Protective Measures:

Review and implement TCG publications:

1. TPM 2.0 Library Specifications v1.83 Errata Version 2.0 or higher. Section 2.2 applies to CVE-2025-2884 (OOB Read).

2. TPM 2.0 Library Specifications v1.59 Errata Version 1.7 or higher. Section 2.7 applies to CVE-2025-2884 (OOB Read).

3. TPM 2.0 Library Specifications v1.38 Errata Version 1.15 or higher. Section 2.38.4 applies to CVE-2025-2884 (OOB Read).

Acknowledgment:

The vulnerabilities were found by an external researcher and reported to the TCG VRT and subsequently coordinated with CERT Coordination Center (CERT/CC). The TCG VRT would like to thank the external researcher and the CERT/CC for a coordinated vulnerability disclosure with TPM Vendors and the ecosystem.

The CERT/CC Vulnerability Note can be found at: https://kb.cert.org/vuls/id/282450