Title: TPM 2.0 library memory corruption vulnerabilities

ID: TCGVRT0007

Released: 2023-FEB-28

Overview:

Vulnerabilities were found in the TPM 2.0 reference implementation code published by the Trusted Computing Group, Revisions 1.59, 1.38 and 1.16 which could potentially result in information disclosure or escalation of privilege.

(https://trustedcomputinggroup.org/resource/tpm-library-specification/) is prone to two potential vulnerabilities, as initially identified by security researchers from Quarks Lab. The reported vulnerabilities occur when handling malicious TPM 2.0 commands with encrypted parameters. Both vulnerabilities are in the `CryptParameterDecryption` function, which is defined in the [Part 4: Supporting Routines – (Code] (https://trustedcomputinggroup.org/wp-content/uploads/TCG_TPM2_r1p59_Part4_SuppRoutines_code_pub.pdf) document, section "10.2.6.6.6 - CryptParameterDecryption()". One of the vulnerabilities is an out-of-bounds read identified as CVE-2023-1018 . The second one is an out-of-bounds write identified as CVE-2023-1017. These vulnerabilities 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. Additional instances may be identified because of the TPM Work Group ongoing analysis and may result in a larger scope of potential vulnerabilities included in TCGVRT0007.

Description:

The reference code did not implement appropriate length checks resulting in potential buffer overflows. The buffer overflows occur on the buffer passed to the ExecuteCommand() entry point (detailed in Part 4 of the spec.) CVE-2023-1017 may allow an attacker to write 2 bytes past the end of that buffer. Those 2 bytes can be written, with attacker-specified values, and therefore the impact assessment depends on what is at that memory location, which may vary across various TPM implementations & vendors. In some implementations the two bytes in question may be unused memory (e.g. in case of certain static buffers), or it could have live data (e.g. if the buffer is on the stack.) CVE-2023-1018 may allow an attacker to read 2 bytes past the end of that buffer.

Impact:

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

Solution and Protective Measures:

Review and implement TCG publications:

1. TPM 2.0 library Specifications v1.59 Errata Version 1.4 or higher. Section 2.6.1 applies to both CVE-2023-1017 (OOB Write) and CVE-2023-1018 (OOB Read). Section 2.6.2 addresses CVE-2023-1018 (OOB Read)). Section 2.6.3 addresses CVE-2023-1017 (OOB Write).
2. TPM 2.0 library Specifications v1.38 Errata Version 1.13 or higher. Section 2.38.1 applies to both CVE-2023-1017 (OOB Write) and CVE-2023-1018 (OOB Read). Section 2.38.2 addresses CVE-2023-1018 (OOB Read). Section 2.38.3 addresses CVE-2023-1017 (OOB Write).
3. TPM 2.0 library Specifications v1.16 Errata Version 1.6 or higher. Section 2.31.1 applies to both CVE-2023-1017 (OOB Write) and CVE-2023-1018 (OOB Read). Section 2.31.2 addresses CVE-2023-1018 (OOB Read).

Acknowledgment: The vulnerabilities were found by Francisco Falcon from Quarkslab and reported to the CERT Coordination Center (CERT/CC) and subsequently reported to the TCG VRT. Additional instances affecting the reference code were found by Vadim Sukhomlinov of Google. The TCG VRT would like to thank Francisco Falcon, Vadim Sukhomlinov 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/782720