Title: TPM 2.0 RSA OAEP Timing Side-Channel Vulnerability

ID: TCGVRT0011

Released: 2026-AUG-11

CVE Identifier: CVE-2026-6727

Weakness: CWE-208: Observable Timing Discrepancy

CVSS:

CVSS v3.1 Base Score: 6.0 Medium

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

CVSS 4.0 Base Score: 8.3 High

Vector: CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N

Overview:

A timing side-channel vulnerability was discovered in the TCG TPM 2.0 reference code affecting all revisions up to and including v184 (2025). This flaw exposes a timing side-channel in RSA OAEP decryption, enabling an attacker to decrypt sensitive blobs (import blobs, credential blobs, and session salts) encrypted to TPM-managed RSA keys, including the RSA Endorsement Key (EK), or to falsify TPM 2.0 Attestation Keys. The vulnerability is rooted in the implementation of OAEP padding checks, which can be exploited using repeated requests and timing analysis (Manger's attack).

Description:

The TPM 2.0 reference code's RSA OAEP decryption routine leaks timing information during padding validation. An adversary can exploit this by sending repeated decryption requests to the TPM and analyzing the response times. This enables a padding oracle attack (Manger's attack), allowing the attacker to decrypt RSA-wrapped credentials, import blobs, or session salts intended for the TPM. The attack is feasible for a local adversary with elevated privileges and knowledge of the TPM's performance characteristics.

Impact:

An adversary can use this vulnerability to:

- Decrypt RSA-wrapped credentials from a TPM Attestation CA for a falsified Attestation Key (with the private key known to the adversary rather than protected by the TPM).

- Falsify other TPM attestations (e.g., PCR quotes for health attestation).
- Decrypt RSA-wrapped import blobs, gaining direct access to sensitive portions (e.g., private keys) of imported objects.
- Decrypt RSA-wrapped session salts, enabling man-in-the-middle attacks against callers establishing salted sessions.

This undermines the confidentiality and integrity of TPM-based trust, impacting device onboarding, secure boot, remote attestation, and session security.

Solution and Protective Measures:

TPM Implementors

Review and implement TCG Publications

1. TPM 2.0 Library Specifications v184 Errata Version 1 or higher.
2. TPM 2.0 Library Specifications v1.83 Errata Version 3 or higher.
3. TPM 2.0 Library Specifications v1.59 Errata Version 1.8 or higher.
4. TPM 2.0 Library Specifications v1.38 Errata Version 1.16 or higher.
5. TPM 2.0 Library Specifications v1.16 Errata Version 1.8 or higher.

Relevant section: “RSA-OAEP decode”

TPM Verifiers

Owners of TPM verifiers should plan to distrust RSA EKs in general in favor of ECC EKs, which are broadly available in current market products.

In environments where RSA EKs must still be used, verifiers should consider allow-listing specific TPM implementations that are not affected. The TPM factory firmware version information is included in the EK certificate extensions. For TPM implementations that are affected and fixed through firmware update, it is strongly recommended revoke all attestations keys and regenerate new attestation certificates after firmware update. Additionally, for TPM implementations that are affected and could not be fixed, TPM verifiers may use known performance characteristics of RSA decryption on those particular models to choose protocol deadlines that make it impractical for an adversary to complete the Manger's attack in time to respond to the verifier.

Acknowledgement:

The vulnerabilities were found by Shai Sarfati and Yanai Moyal from Intel.

The TCG VRT thanks 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/43103

References:

VRT0010/VRT0011 Extended Guidance Document

https://kb.cert.org/vuls/id/43103

https://www.cve.org/CVERecord?id=CVE-2026-6727