# CVE Detail – CVE-2020-12926

The Trusted Platform Modules (TPM) reference software may not properly track the number of times a failed shutdown happens. This can leave the TPM in a state where confidential key material in the TPM may be able to be compromised. AMD believes that the attack requires physical access of the device because the power must be repeatedly turned on and off. This potential attack may be used to change confidential information, alter executables signed by key material in the TPM, or create a denial of service of the device.

## Threat-Mapped Scoring

Score: 1.5

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.12771

## CVSS Scoring

CVSS v3.1 Score: 6.4

Severity: MEDIUM

## Mapped CWE(s)

* CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition

## CAPEC(s)

* CAPEC-27: Leveraging Race Conditions via Symbolic Links
* CAPEC-29: Leveraging Time-of-Check and Time-of-Use (TOCTOU) Race Conditions

## Affected Products

* cpe:2.3:a:amd:trusted\_platform\_modules\_reference:-:\*:\*:\*:\*:\*:\*:\*