# CVE Detail – CVE-2023-1017

An out-of-bounds write vulnerability exists in TPM2.0's Module Library allowing writing of a 2-byte data past the end of TPM2.0 command in the CryptParameterDecryption routine. An attacker who can successfully exploit this vulnerability can lead to denial of service (crashing the TPM chip/process or rendering it unusable) and/or arbitrary code execution in the TPM context.

## Threat-Mapped Scoring

Score: 1.9

Priority: P3 - Important (Medium)

## EPSS

EPSS Score: N/A

Percentile: 0.44343

## CVSS Scoring

CVSS v3.1 Score: 7.8

Severity: HIGH

## Mapped CWE(s)

* CWE-787: Out-of-bounds Write

## Affected Products

* cpe:2.3:a:trustedcomputinggroup:trusted\_platform\_module:2.0:revision\_1.16:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:trustedcomputinggroup:trusted\_platform\_module:2.0:revision\_1.38:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:trustedcomputinggroup:trusted\_platform\_module:2.0:revision\_1.59:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:microsoft:windows\_10\_1507:\*:\*:\*:\*:\*:\*:x64:\*
* cpe:2.3:o:microsoft:windows\_10\_1607:\*:\*:\*:\*:\*:\*:x64:\*
* cpe:2.3:o:microsoft:windows\_10\_1809:\*:\*:\*:\*:\*:\*:x64:\*
* cpe:2.3:o:microsoft:windows\_10\_20h2:\*:\*:\*:\*:\*:\*:x64:\*
* cpe:2.3:o:microsoft:windows\_10\_21h2:\*:\*:\*:\*:\*:\*:x64:\*
* cpe:2.3:o:microsoft:windows\_10\_22h2:\*:\*:\*:\*:\*:\*:x64:\*
* cpe:2.3:o:microsoft:windows\_11\_21h2:\*:\*:\*:\*:\*:\*:x64:\*
* cpe:2.3:o:microsoft:windows\_11\_22h2:\*:\*:\*:\*:\*:\*:x64:\*
* cpe:2.3:o:microsoft:windows\_server\_2016:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:microsoft:windows\_server\_2019:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:microsoft:windows\_server\_2022:\*:\*:\*:\*:\*:\*:\*:\*