CVE-2023-1018

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2023-1018
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-02-28 18:15:00 UTC
Updated	2024-04-01 15:50:00 UTC
Description	An out-of-bounds read vulnerability exists in TPM2.0's Module Library allowing a 2-byte read past the end of a TPM2.0 com

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 10 1507	All	All	All	All
Operating System	Microsoft	Windows 10 1607	All	All	All	All
Operating System	Microsoft	Windows 10 1809	All	All	All	All
Operating System	Microsoft	Windows 10 20h2	All	All	All	All
Operating System	Microsoft	Windows 10 21h2	All	All	All	All
Operating System	Microsoft	Windows 10 22h2	All	All	All	All
Operating System	Microsoft	Windows 11 21h2	All	All	All	All
Operating System	Microsoft	Windows 11 22h2	All	All	All	All
Operating System	Microsoft	Windows Server 2016	All	All	All	All
Operating System	Microsoft	Windows Server 2019	All	All	All	All
Operating System	Microsoft	Windows Server 2022	All	All	All	All
Application	Trustedcomputinggroup	Trusted Platform Module	2.0	revision_1.16	All	All
Application	Trustedcomputinggroup	Trusted Platform Module	2.0	revision_1.38	All	All
Application	Trustedcomputinggroup	Trusted Platform Module	2.0	revision_1.59	All	All

References

Reference	Source	Link	Tags

VU#782720 - TCG TPM2.0 implementations vulnerable to memory corruption	MISC	kb.cert.org	
Security | Trusted Computing Group	MISC	trustedcomputinggroup.org	
trustedcomputinggroup.org/wp-content/uploads/TCGVRT0007-Advisory-FINAL.pdf	MISC	trustedcomputinggroup.org	
Errata for TPM Library Specification 2.0 | Trusted Computing Group	MISC	trustedcomputinggroup.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ana

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 160624 Oracle Enterprise Linux Security Update for libtpms (ELSA-2023-2453)
- 160683 Oracle Enterprise Linux Security Update for virt:ol and virt-devel:rhel (ELSA-2023-2757)
- 182913 Debian Security Update for libtpms (CVE-2023-1018)
- 199222 Ubuntu Security Notification for Libtpms Vulnerabilities (USN-5933-1)
- 241358 Red Hat Update for virt:rhel and virt-devel:rhel (RHSA-2023:1833)
- 241437 Red Hat Update for libtpms (RHSA-2023:2453)
- 241506 Red Hat Update for virt:rhel and virt-devel:rhel security (RHSA-2023:2757)
- 283760 Fedora Security Update for libtpms (FEDORA-2023-c487bde4b4)
- 283795 Fedora Security Update for libtpms (FEDORA-2023-4afddd37a9)
- 284266 Fedora Security Update for libtpms (FEDORA-2023-64f2a84db1)
- 378058 TPM 2.0 library memory corruption vulnerabilities (TCGVRT0007)
- 378706 Alibaba Cloud Linux Security Update for virt:rhel and virt-devel:rhel (ALINUX3-SA-2023:0082)
- 753950 SUSE Enterprise Linux Security Update for libtpms (SUSE-SU-2023:2051-1)
- 91990 Microsoft Windows Security Update for March 2023
- 91996 Microsoft Azure Stack Hub Security Updates for March 2023
- 941022 AlmaLinux Security Update for libtpms (ALSA-2023:2453)
- 941115 AlmaLinux Security Update for virt:rhel and virt-devel:rhel (ALSA-2023:2757)

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report