Out-of-Bounds read vulnerability in TCG TPM2.0 reference implementation

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2025-2884
State	PUBLISHED
Assigner	certcc
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-06-10 18:15:30 UTC
Updated	2026-04-14 10:16:26 UTC
Description	TCG TPM2.0 Reference implementation's CryptHmacSign helper function is vulnerable to Out-of-Bounds read due to the la

Risk And Classification

Primary CVSS: v3.1 6.6 MEDIUM from ADP

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

EPSS: 0.000720000 probability, percentile 0.218390000 (date 2026-04-15)

Problem Types: CWE-125 | CWE-125 Out-of-bounds Read | CWE-125 CWE-125 Out-of-bounds Read

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	6.6	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	6.6	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Unchanged

Confidentiality

High

ntegrity

None

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Trusted Computing Group	TPM2.0	affected 1.83 custom	Not specified
ADP	Siemens	SIMATIC CN 4100	affected * custom	Not specified
ADP	Siemens	SIMATIC Field PG M5	affected * custom	Not specified
ADP	Siemens	SIMATIC Field PG M6	affected * custom	Not specified
ADP	Siemens	SIMATIC IPC BX-32A	affected V29.01.09 custom	Not specified
ADP	Siemens	SIMATIC IPC BX-39A	affected V29.01.09 custom	Not specified
ADP	Siemens	SIMATIC IPC BX-56A	affected V32.01.09 custom	Not specified
ADP	Siemens	SIMATIC IPC BX-59A	affected V32.01.09 custom	Not specified
ADP	Siemens	SIMATIC IPC MD-57A	affected V30.01.10 custom	Not specified
ADP	Siemens	SIMATIC IPC PX-32A	affected V29.01.09 custom	Not specified
ADP	Siemens	SIMATIC IPC PX-39A	affected V29.01.09 custom	Not specified
ADP	Siemens	SIMATIC IPC PX-39A PRO	affected V29.01.09 custom	Not specified
ADP	Siemens	SIMATIC IPC RW-528A	affected V34.01.02 custom	Not specified
ADP	Siemens	SIMATIC IPC RW-548A	affected V34.01.02 custom	Not specified
ADP	Siemens	SIMATIC IPC227E	affected * custom	Not specified
ADP	Siemens	SIMATIC IPC277E	affected * custom	Not specified
ADP	Siemens	SIMATIC IPC427E	affected V21.01.20 custom	Not specified
ADP	Siemens	SIMATIC IPC477E	affected V21.01.20 custom	Not specified
ADP	Siemens	SIMATIC IPC477E PRO	affected V21.01.20 custom	Not specified
ADP	Siemens	SIMATIC IPC627E	affected * custom	Not specified
ADP	Siemens	SIMATIC IPC647E	affected * custom	Not specified
ADP	Siemens	SIMATIC IPC677E	affected * custom	Not specified
ADP	Siemens	SIMATIC IPC847E	affected * custom	Not specified
ADP	Siemens	SIMATIC ITP1000	affected * custom	Not specified
ADP	Siemens	SIPLUS IPC427E	affected V21.01.20 custom	Not specified

References

Reference	Source
github.com/stefanberger/libtpms/commit/04b2d8e9afc0a9b6bffe562a23e58c0de...	cret@cert.org
www.kb.cert.org/vuls/id/282450	af854a3a-2127-422b-91ae-364da2661108
trustedcomputinggroup.org/about/security	cret@cert.org
www.cve.org/CVERecord	cret@cert.org
cert-portal.siemens.com/productcert/html/ssa-628843.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e
www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01209.html	af854a3a-2127-422b-91ae-364da2661108
trustedcomputinggroup.org/wp-content/uploads/TPM2.0-Library-Spec-v1.83-Errata_v1_pub.pdf	cret@cert.org
trustedcomputinggroup.org/wp-content/uploads/VRT0009-Advisory-FINAL.pdf	cret@cert.org
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.