

CVE-2026-98728

Microsoft tpm: fix off-by-four bounds check in tpm2_get_random()

In the Linux kernel, the following vulnerability has been resolved: tpm: fix off-by-four bounds check in tpm2_get_random()
When the response carries the TPM2_ST_SESSIONS tag, tpm2_get_random() skips the 4-byte parameter size field before locating the random data, but the bounds check still validates the response length against TPM_HEADER_SIZE. A truncated response can pass the check and make memcpy() read up to 4 bytes past the response end, so stale buffer contents end up in the caller's random bytes.

EVRS 0 /100 Informational priority	CVSS — Not scored	EPSS 0.002 5.7th percentile · FIRST	CISA DEADLINE — No CISA deadline
---	-------------------------	--	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 2 of 8 signals

☐ CISA KEV	Not currently CISA KEV-listed	☐ Vendor exploitation	Active-exploitation status not yet checked - scored at the population base rate (none) until known
☐ Ransomware	Ransomware association unavailable	☐ KEV recency	CISA KEV listing date unavailable
☐ EPSS	0.002 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☐ CVSS	CVSS base score unavailable	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Monitor Untagged reference available; patch status is not confirmed

NVD lists one or more references for this CVE that aren't tagged as a patch or vendor advisory. Review them directly to confirm patch availability and applicability before making a remediation decision.

Basis: NVD reference (untagged)

Fix this by checking the response length against 'offset', which already includes the skipped parameter size field.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
Not identified by the connected sources	—	no fixed version listed	NVD

Sources

Reference	git.kernel.org/stable/c/42bb6216b861e892512128219ff23010d656ba14	Additional reference	git.kernel.org/stable/c/9b522400bf5c082feb9a0037a053ea822a2c7e4d
Additional reference	git.kernel.org/stable/c/be54101992c2c5218be0e0a87827ccc96e3089af	Additional reference	git.kernel.org/stable/c/e30a2406408d2df6d9cd48c2e59e913cf266a05a
NVD	nvd.nist.gov/vuln/detail/CVE-2026-98728	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103813
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98728		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.