

CVE-2026-98724

Microsoft nvmet: pci-epf: reject too-short SGL segments

In the Linux kernel, the following vulnerability has been resolved: nvmet: pci-epf: reject too-short SGL segments The host controls an SGL segment's length. A nonzero length smaller than one SGL descriptor makes nr_descs zero, so nvmet_pci_epf_get_sgl_segment() reads the type byte of sgls[-1] outside the allocated buffer. If that byte contains a segment descriptor type, the function also copies the preceding 16 bytes and returns a negative descriptor count.

EVRS 0 /100 Informational priority	CVSS — Not scored	EPSS 0.002 9th 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)

The read was reproduced in 3/3 KASAN boots with only the host transfer mocked by a KUnit test: BUG: KASAN: slab-out-of-bounds in nvmet_pci_epf_get_sgl_segment Read of size 1 by task kunit_try_catch Call Trace: nvmet_pci_epf_get_sgl_segment nvmet_pci_epf_short_sgl_test Kernel panic - not syncing: KASAN: panic_on_warn set ... Reject segments that cannot hold one descriptor before allocating or transferring their contents.

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/2423a05dd0f21330c47ce0ae1cb54a8b0be821e2	Additional reference	git.kernel.org/stable/c/472df1d103dbe3e9d09156f0667e36180e912c46
Additional reference	git.kernel.org/stable/c/5d5fbfbaccd1efb13a9bf91317d4fde859ede4b9	NVD	nvd.nist.gov/vuln/detail/CVE-2026-98724
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103809	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98724

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