

CVE-2026-98723

Microsoft nvmet: copy the hostid into the ctrl before creating PR pc_refs

In the Linux kernel, the following vulnerability has been resolved: nvmet: copy the hostid into the ctrl before creating PR pc_refs
Commit 6202783184bf ("nvmet: Improve nvmet_alloc_ctrl() interface and implementation") added a second uuid_copy() of args->hostid near the end of nvmet_alloc_ctrl(), and commit 7b658153f1b8 ("nvmet: Remove duplicate uuid_copy") removed the original copy that sat before nvmet_ctrl_init_pr() instead of the new one.

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)

Since then nvmet_ctrl_init_pr() snapshots ctrl->hostid into the per-controller per-namespace reservation refs while the uuid_copy() from the connect data runs later, after the controller is published. The ctrl is allocated with kzalloc(), so every pc_ref created on this path stores the nil UUID. pc_ref->hostid has a single consumer: nvmet_pr_set_ctrl_to_abort() matches it against the preempted registrant's hostid to kill and drain the victim's in-flight I/O for Preempt and Abort. The match can never hit with the nil UUID, so whenever a namespace with reservations enabled exists before a host connects, which includes every reconnect, Preempt and Abort silently degrades into a plain Preempt: the preempting host sees success while the victim's in-flight I/O is still in the air. Copy the hostid where the rest of the connect data is consumed, before the controller is published and before nvmet_ctrl_init_pr() takes its snapshot.

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/23194531595c5d1d4454e3a607b0c8fc0c4e8695	Additional reference	git.kernel.org/stable/c/5211fed41d7ec90e9ab7239dc4bffffe4d0b2b62
Additional reference	git.kernel.org/stable/c/d3d6d7efdacc08616d23b3ac42272a494951dc0f	NVD	nvd.nist.gov/vuln/detail/CVE-2026-98723
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103977	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98723

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