

CVE-2026-98727

Microsoft nvme-multipath: set BLK_FEAT_ZONED only after the zone info is known

In the Linux kernel, the following vulnerability has been resolved: nvme-multipath: set BLK_FEAT_ZONED only after the zone info is known The namespace head is marked zoned at allocation time based only on the command set identifier. If the zone info query reports a zero zone size, the path namespace is registered without zoned limits while the head still advertises the zoned capability with a zone size of zero, and reporting zones or writing to the head then shifts by `ilog2(0)`.

EVRS 0 /100 Informational priority	CVSS — Not scored	EPSS 0.002 9.3rd 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)

Drop the zoned feature from the head allocation and let the head limits refresh stack it in from the path namespace instead.

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/2d86abd28071481a1abd87204a47325975dc821c	Additional reference	git.kernel.org/stable/c/44dc998c38fb5e153c3ed5665f112661841c3f5
Additional reference	git.kernel.org/stable/c/4a5e49ba0abb8b4328d6318c9aef0c0121f95507	Additional reference	git.kernel.org/stable/c/8b85838c1fdb5a90152693ca158aa9660c628f
NVD	nvd.nist.gov/vuln/detail/CVE-2026-98727	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103812
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98727		

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