

CVE-2026-98867

Microsoft dm-pcache: bound the logical key offset from persistent memory

In the Linux kernel, the following vulnerability has been resolved: dm-pcache: bound the logical key offset from persistent memory cache_key_decode() takes a key's logical off from the cache device and later indexes req_key_tree->subtrees[] by it in get_subtree(). An off past the device forms a subtree pointer outside the array, which rb_insert() writes through during replay. Reject a key of zero length, or whose off+len (computed in 64 bits) exceeds the device size, before it is used.

EVRS 0 /100 Informational priority	CVSS — Not scored	EPSS 0.002 4.2nd 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)

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/10449703200076980704894c3d68d6796182371b	Additional reference	git.kernel.org/stable/c/3d5a87cb909c1f375f08065b20123fa5db5958d8
Additional reference	git.kernel.org/stable/c/97fc4b53dbe4a983fdf093243067fa6a64562307	NVD	nvd.nist.gov/vuln/detail/CVE-2026-98867
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103807	Current data	evulnabile.com/vulnerability-management/cve/CVE-2026-98867

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