

CVE-2026-98843

Microsoft netfs: zero gaps in read-gaps folio to avoid writing back stale data

In the Linux kernel, the following vulnerability has been resolved: netfs: zero gaps in read-gaps folio to avoid writing back stale data netfs_read_gaps() leaves gaps around a streaming write's dirty region unread on the server side, so a short/EOF response there left stale folio content that later got written back. Zero it after the read completes, not before: netfs_wait_for_read() returns rreq->transferred once ret >= 0, so build an iterator over the same bvec array the read used, advance past ret, and zero the

EVRS 0 /100 Informational priority	CVSS — Not scored	EPSS 0.002 5.5th percentile · FIRST	CISA DEADLINE — No CISA deadline
---	-------------------------	--	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 2 of 8 signals

☐ CISA KEY	Not currently CISA KEY-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)

rest. The dirty region already maps to sink pages in that array rather than the real folio, so this can't touch it, and only the actual shortfall gets zeroed instead of the whole gap upfront.

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/2a62fe628a877c249c8286b157ee99d82840d9dc	Additional reference	git.kernel.org/stable/c/512eaf01ffabf4258e945016b50df5aed940b705
Additional reference	git.kernel.org/stable/c/8db55c5cd831a786a1a2a2d391aa80354535a353	NVD	nvd.nist.gov/vuln/detail/CVE-2026-98843
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103783	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98843

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