

CVE-2026-98684

Microsoft smb: client: flush and commit data before querying allocated ranges

In the Linux kernel, the following vulnerability has been resolved: smb: client: flush and commit data before querying allocated ranges The mode 0 / FALLOC_FL_KEEP_SIZE fallocate emulation for small interior ranges in smb3_simple_fallocate_range() issues FSCTL_QUERY_ALLOCATED_RANGES and zero-fills any sub-range the server reports as an unallocated hole, to force block allocation without changing file contents. This is unsafe against Windows servers.

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 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)

Per the Win32 documentation, FSCTL_QUERY_ALLOCATED_RANGES only reports ranges that *may* contain nonzero data and is explicitly not coherent with recently written data: "a call to FSCTL_QUERY_ALLOCATED_RANGES [after writing to a network file] would not necessarily return a correct list of allocated regions. To ensure coherency [...] flush the data to the file" fsx (generic/363) reproduces the resulting corruption against Windows Server 2022: a range is written, an uncached read returns the data, yet the next FSCTL_QUERY_ALLOCATED_RANGES on that range reports it as a whole hole, so the emulation overwrites live data with zeroes. A network trace confirmed the WRITE, the READ returning data and the query returning an empty range list within microseconds. Samba does not exhibit this; its query is coherent with the written data. Write back the dirty pages, drain any outstanding I/O and issue an SMB2 FLUSH to force the server to commit the data before querying the allocated ranges, so the query reflects the data actually present. With this, generic/363 passes against both Windows Server 2022 and Samba over 100000 fsx operations.

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/aa994489bd835547c191827acc460192e147032d	Additional reference	git.kernel.org/stable/c/bf84e44ff0ed802778eafd7ecb623635379cb506
Additional reference	git.kernel.org/stable/c/f82242fe3109a3ef72f429540b5bdde08fbfb0e4	NVD	nvd.nist.gov/vuln/detail/CVE-2026-98684
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103938	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98684

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