

CVE-2026-98445

Microsoft xfs: don't let memory failures leak blocks and kill repairs

In the Linux kernel, the following vulnerability has been resolved: xfs: don't let memory failures leak blocks and kill repairs
LOLLM complains that a memory allocation failure in xrep_newbt_add_blocks results in online repair leaking blocks that were previously allocated to write a new btree, but the problem is worse than that -- a limitation of the codebase is that the callers cannot undo the transaction /and/ return the error -- either you undo all changes and commit the transaction, or you error out and the

EVRS	CVSS	EPSS	CISA DEADLINE
0/100 Informational priority	— Not scored	0.002 5.7th percentile · FIRST	— 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)

filesystem goes down. However, the new btree space reservation object isn't that big (~48 bytes). Let's just do a NOFAIL allocation and the problem goes away.

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/0e0d3372a84029da1768c7a4c4601484af5b58a2	Additional reference	git.kernel.org/stable/c/3380151cf0ce8ad0c1d356fed51e4b69e1d28e50
Additional reference	git.kernel.org/stable/c/ab1c416d2377cdc16123ef521aac4da1c468c3d4	Additional reference	git.kernel.org/stable/c/b15c79fca28060fd9c7e77f2c3ebc4ba023974e8
NVD	nvd.nist.gov/vuln/detail/CVE-2026-98445	ENISA EUVD	euid.enisa.europa.eu/vulnerability/EUVD-2026-103685
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98445		

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