CVE-2026-98223

Microsoft mm: filemap: retain mapped dropbehind folios

In the Linux kernel, the following vulnerability has been resolved: mm: filemap: retain mapped dropbehind folios Fault-around can map ready dropbehind folios without going through the normal page-cache lookup that clears dropbehind. A mapping represents a competing cached user, so retain the folio instead of forcibly unmapping it when writeback completes. For a mapped folio, folio_unmap_invalidate() can call unmap_mapping_folio(), which takes i_mmap_rwsem and may sleep.

EVRS	CVSS	EPSS	CISA DEADLINE
0/100 Informational priority	— Not scored	0.002 6.4th 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
Ransomware	Ransomware association unavailable
EPSS	0.002 probability
CVSS	CVSS base score unavailable
Vendor exploitation	Active-exploitation status not yet checked - scored at the population base rate (none) until known
KEV recency	CISA KEV listing date unavailable
Pre-patch disclosure	Disclosure status 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)

Retaining mapped folios avoids this path when folio_end_dropbehind() runs in non-preemptible task context. Tal was able to trigger a sleeping-in-atomic warning due to this [1]. Unmapped dropbehind folios continue through the existing invalidation path.

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/2897601dffe576fcd87a4259102f41f7fb0cbfc8	Additional reference	git.kernel.org/stable/c/77c0fade37c80e8aa16ac048a9828249055e3f66
Additional reference	git.kernel.org/stable/c/848d2ce2fce15fbdc083fbf9691bfa72911033c4	NVD	nvd.nist.gov/vuln/detail/CVE-2026-98223
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-93151	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98223

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