

# 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<br><b>0</b> /100<br>Informational priority | CVSS<br>—<br>Not scored | EPSS<br><b>0.002</b><br>6.4th percentile · FIRST | CISA DEADLINE<br>—<br>No CISA deadline |
|-------------------------------------------------|-------------------------|--------------------------------------------------|----------------------------------------|

## Signals behind the score

☒ counted in the score ☐ not counted

evidence for 2 of 8 signals

|                                            |                                    |                                                                |                                                                                                    |
|--------------------------------------------|------------------------------------|----------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> <b>CISA KEV</b>   | Not currently CISA KEV-listed      | <input type="checkbox"/> <b>Vendor exploitation</b>            | Active-exploitation status not yet checked - scored at the population base rate (none) until known |
| <input type="checkbox"/> <b>Ransomware</b> | Ransomware association unavailable | <input type="checkbox"/> <b>KEV recency</b>                    | CISA KEV listing date unavailable                                                                  |
| <input type="checkbox"/> <b>EPSS</b>       | 0.002 probability                  | <input type="checkbox"/> <b>Pre-patch disclosure</b>           | Disclosure status unavailable                                                                      |
| <input type="checkbox"/> <b>CVSS</b>       | CVSS base score unavailable        | <input type="checkbox"/> <b>Microsoft Exploitability Index</b> | 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            | <a href="https://git.kernel.org/stable/c/2897601dffe576fcd87a4259102f41f7fb0cbfc8">git.kernel.org/stable/c/2897601dffe576fcd87a4259102f41f7fb0cbfc8</a> | Additional reference | <a href="https://git.kernel.org/stable/c/77c0fade37c80e8aa16ac048a9828249055e3f66">git.kernel.org/stable/c/77c0fade37c80e8aa16ac048a9828249055e3f66</a> |
| Additional reference | <a href="https://git.kernel.org/stable/c/848d2ce2fce15fbdc083fbf9691bfa72911033c4">git.kernel.org/stable/c/848d2ce2fce15fbdc083fbf9691bfa72911033c4</a> | NVD                  | <a href="https://nvd.nist.gov/vuln/detail/CVE-2026-98223">nvd.nist.gov/vuln/detail/CVE-2026-98223</a>                                                   |
| ENISA EUVD           | <a href="https://euvd.enisa.europa.eu/vulnerability/EUVD-2026-93151">euvd.enisa.europa.eu/vulnerability/EUVD-2026-93151</a>                             | Current data         | <a href="https://evulnable.com/vulnerability-management/cve/CVE-2026-98223">evulnable.com/vulnerability-management/cve/CVE-2026-98223</a>               |

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