

CVE-2026-98224

Microsoft mm/vma: correctly unaccount on mmap_prepare() failure

In the Linux kernel, the following vulnerability has been resolved: mm/vma: correctly unaccount on mmap_prepare() failure
__mmap_setup() accounts memory for relevant mappings via: security_vm_enough_memory_mm() -> __vm_enough_memory()
-> vm_acct_memory() If __mmap_setup() fails, this indicates that this accounting did not take place, and thus it's appropriate for __mmap_region() to jump to abort_munmap. However if call_mmap_prepare() fails, it also jumps there and any accounted memory is not correctly unaccounted. Fix this by handling each error separately.

EVRS 0 /100 Informational priority	CVSS — Not scored	EPSS 0.002 6.4th 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)

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/6cc27d82196385fe06853319f74312a7d8019726	Additional reference	git.kernel.org/stable/c/8fdc521d438fbf0d22c13d51d55d5dd82d7202b2
Additional reference	git.kernel.org/stable/c/fb5400bff669c8bad3d4ec09287d9b461e89e5f1	NVD	nvd.nist.gov/vuln/detail/CVE-2026-98224
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-93152	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98224

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