

CVE-2026-98729

Microsoft x86/mm: Don't apply va_align to hugetlb mappings on AMD F15h

In the Linux kernel, the following vulnerability has been resolved: x86/mm: Don't apply va_align to hugetlb mappings on AMD F15h get_align_mask() returns huge_page_mask_align() for hugetlbfs, but get_align_bits() adds va_align.bits regardless, so vm_unmapped_area() returns an address off the huge page boundary and __unmap_hugepage_range() hits BUG_ON(start & ~huge_page_mask(h)) at teardown. This can be triggered on Carrizo and FX-8370E, both hstates. Pass the file to get_align_bits() and skip the randomisation for hugetlbfs. [bp: Message commit message.]

EVRS	CVSS	EPSS	CISA DEADLINE
0/100	—	0.002	—
Informational priority	Not scored	5.5th 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)

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/b46b2e2de47ca9449532b0a7110ed99f79061d6e	Additional reference	git.kernel.org/stable/c/d2457a7e2727dc747a61a50d65c2f259afce8c45
Additional reference	git.kernel.org/stable/c/fe23680e6f1d52b8cc45d77bf7c54249508a81c7	NVD	nvd.nist.gov/vuln/detail/CVE-2026-98729
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103814	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98729

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