

CVE-2026-98475

Microsoft s390/cmf: Fix virtual vs physical address confusion

In the Linux kernel, the following vulnerability has been resolved: s390/cmf: Fix virtual vs physical address confusion The measurement block address is an absolute address. Define the associated schib_config and schib fields as dma64_t to enable automatic detection of incorrect assignments. Also add the missing virt_to_dma64() translation. Without this fix, a wrong address will be used by firmware when storing extended format channel measurement data on kernels built with CONFIG_RANDOMIZE_IDENTITY_BASE=y.

EVRS 0 /100 Informational priority	CVSS — Not scored	EPSS 0.002 5.7th 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/748ec2f7f5df9b4fc742546a8bfc8aa5d847353e	Additional reference	git.kernel.org/stable/c/7f78226eb743b362f52b212d7763801642539d1c
Additional reference	git.kernel.org/stable/c/b11f369be31ea11c746833e4d3ad51dcd6b5fa2b	Additional reference	git.kernel.org/stable/c/f4d04425e66af2ecee9d1a49ae0484436f3c2fd1
NVD	nvd.nist.gov/vuln/detail/CVE-2026-98475	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103715
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98475		

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