

CVE-2026-98713

Microsoft KVM: arm64: Apply the fine-grained UNDEFs without FEAT_FGT

In the Linux kernel, the following vulnerability has been resolved: KVM: arm64: Apply the fine-grained UNDEFs without FEAT_FGT FGUs don't actually require hardware support, so don't gate fgt trap config insertion on FGT. This is the only action required to allow FGUs always, as kvm_calculate_traps() already computes the FGU bits with or without FEAT_FGT. This also fixes a spurious WARN when a TLBI OS is run on a guest in vEL1 without FEAT_TLBIOS on non FEAT_FGT hardware.

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 KEY	Not currently CISA KEY-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 KEY 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)

In this configuration the course-grained HCR_EL2.TTBR0S trap reaches the handler handle_tlb_el1(), which expects an EL1 TLBI only from vEL2. With FGUs enabled the UNDEF will be injected without needing the specific handler. [oliver: Take Wei-Lin's suggested changelog]

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/1113374a17d7f7d16b02ee0bbd9b1e7a60cbb087	Additional reference	git.kernel.org/stable/c/2f4a15c52a552c5244ec27f4ca8bda855594f918
Additional reference	git.kernel.org/stable/c/4bdd2b3a708c1feb701cb8b62feb8ad2fd77bb07	Additional reference	git.kernel.org/stable/c/af3300b3a6bace925a496f3520e171c07b999c72
NVD	nvd.nist.gov/vuln/detail/CVE-2026-98713	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103967
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98713		

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