

CVE-2026-98546

Microsoft arm64/boot: Disable trapping of PMZR_ELO writes to EL2

In the Linux kernel, the following vulnerability has been resolved: arm64/boot: Disable trapping of PMZR_ELO writes to EL2 __init_el2_fgt2() writes one mask to both HDFGRTR2_EL2 and HDFGWTR2_EL2. PMZR_ELO is write-only, so its trap bit, nPMZR_ELO, exists only in HDFGWTR2_EL2 and is therefore never set: a PMZR_ELO write from the host traps to EL2, where the nVHE hypervisor has no handler and BUG(s).

EVRS 0 /100 Informational priority	CVSS — Not scored	EPSS 0.002 9.3rd 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)

The kernel never writes PMZR_ELO, but kernel.perf_user_access=1 has the PMU driver set PMUSERENR_ELO.UEN for a task with a user-read event, so a write from ELO reaches the trap and takes the host down without a panic message. Accumulate the HDFGWTR2_EL2 bits separately, as __init_el2_fgt() already does for HDFGWTR_EL2, and set nPMZR_ELO with the other FEAT_PMUv3p9 bits.

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/071f51188a5d8ec10535541255587976d12fc7d8	Additional reference	git.kernel.org/stable/c/2bc6b218717b9d08f466f88209251d54bc09b207
Additional reference	git.kernel.org/stable/c/bb8c90c86441c090e9036f019cf1b4d7894a2c40	Additional reference	git.kernel.org/stable/c/ce71865bf43f88bed9d9218e9218e537150be506
NVD	nvd.nist.gov/vuln/detail/CVE-2026-98546	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103591
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98546		

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