

CVE-2026-98637

Microsoft KVM: arm64: Do not clear VM-wide SVE feature on vCPU init failure

In the Linux kernel, the following vulnerability has been resolved: KVM: arm64: Do not clear VM-wide SVE feature on vCPU init failure pkvm_vcpu_init_sve() clears KVM_ARM_VCPU_SVE in kvm->arch.vcpu_features when it fails, but vcpu_has_sve() tests KVM_ARCH_FLAG_GUEST_HAS_SVE, which is left set. Later vCPUs on that VM then skip the SVE setup and register with a NULL sve_state, which the guest's first FP access hands to sve_load_state(). Return the error without touching vcpu_features.

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

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/a1b3c788ad31837e348075e93dbba3f447492776	Additional reference	git.kernel.org/stable/c/bd46b41f412fb81c50bac1a0929ec31320f3a807
Additional reference	git.kernel.org/stable/c/f0cd8ffae092cc1b9d7cfa9188ed5a88a374adcb	NVD	nvd.nist.gov/vuln/detail/CVE-2026-98637
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103551	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98637

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