

CVE-2026-98638

Microsoft KVM: arm64: Validate the SVE vector length in pkvm_vcpu_init_sve()

In the Linux kernel, the following vulnerability has been resolved: KVM: arm64: Validate the SVE vector length in pkvm_vcpu_init_sve() pkvm_vcpu_init_sve() clamps only the upper bound of the host-provided sve_max_vl, so an invalid vector length reaches sve_state_size_from_vl() and the WARN_ON() there, which is fatal at EL2. The existing !sve_state_size test rejects such a length, but only after the macro has run. Check sve_vl_valid() before deriving the state size. A valid length cannot yield a zero size, so the !sve_state_size test goes with it.

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 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/2a2eb10795a1e495aebc7f829cceb72c05b4fd9	Additional reference	git.kernel.org/stable/c/bae3e4493046de4fefa15f809d9b8dc114e84a3d
Additional reference	git.kernel.org/stable/c/faf66e55e87498ab4bf88cdf9a629e61b3f2d3bc	NVD	nvd.nist.gov/vuln/detail/CVE-2026-98638
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103552	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98638

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