

CVE-2026-98440

Microsoft KVM: arm64: nv: Delay freeing of shadow S2 structures until VM destruction

In the Linux kernel, the following vulnerability has been resolved: KVM: arm64: nv: Delay freeing of shadow S2 structures until VM destruction We free the shadow S2 structures from kvm_arch_flush_shadow_all(), which is a Bad Idea(tm). Freeing the page tables is fair game (this is what this callback is for), but freeing the container that could still be referenced by another part of the system is not great. Instead, grow separate destructors that gets called when we tear the VM down for good.

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)

From there, we can nuke both the individual MMUs as well as the global array that points to them, safe in the knowledge that the vcpus themselves have been destroyed already.

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/22e82acec93a681071ed36f70eabe2d0c4e0bebd	Additional reference	git.kernel.org/stable/c/5bf1c9175e657b3c2dc1cf77403031ac7aadcf66
Additional reference	git.kernel.org/stable/c/876049f026b4dfaca0cc78ec81be0e639ca8525d	Additional reference	git.kernel.org/stable/c/e5843f4effaa2ffac3e789ecd4456403564961d4
NVD	nvd.nist.gov/vuln/detail/CVE-2026-98440	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103680
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98440		

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