

CVE-2026-98472

Microsoft KVM: SEV: Free have_run_cpus during VM destruction even if VM is no longer SEV

In the Linux kernel, the following vulnerability has been resolved: KVM: SEV: Free have_run_cpus during VM destruction even if VM is no longer SEV Unconditionally free SEV's "have run CPUs" cpumask in the VM destroy path, i.e. even for what appear to be non-SEV VMs, as an SEV VM becomes a non-SEV VM if its state is intra-host migrated. Alternatively, the mask could be freed in sev_migrate_from() when "converting" the source VM, but that gets annoying because ideally KVM would nullify the mask to guard against UAF,

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)

and nullifying the mask would need be conditioned on CPUMASK_OFFSTACK=y. Freeing the mask during sev_migrate_from() is also not robust against other KVM bugs, though that's kind of a moot point since any such bugs would show up even if sev->active is never set. I.e. KVM must get that side of things correct. But, that's not a great reason to add more code just to make things marginally less robust.

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/12c1f6e03f944e399bd2c88441dca5dc702b95a5	Additional reference	git.kernel.org/stable/c/6aef7cf800098749ff5d66022efaf6e01e98c09
Additional reference	git.kernel.org/stable/c/9784e5ca91b37b387f3f414af4340c54f7a63566	NVD	nvd.nist.gov/vuln/detail/CVE-2026-98472
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103712	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98472

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