

CVE-2026-98639

Microsoft KVM: riscv: Fix NACL hfence entry update order

In the Linux kernel, the following vulnerability has been resolved: KVM: riscv: Fix NACL hfence entry update order The SBI v3.0 specification (section 15.1.2) requires a nested HFENCE entry to be populated as follows: 1) find an unused entry with Config.Pending == 0 2) update the Page_Number and Page_Count words 3) update the Config word with Config.Pending set __kvm_riscv_nacl_hfence() writes the Config word first, so the SBI implementation (or NACL hardware) can observe a pending entry with pnun/pcount values

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)

left over from the previous use of that entry, resulting in incorrect TLB flush ranges. Write pnun and pcount first and the Config word last. Since the consumer is an external agent on coherent shared memory, use WRITE_ONCE() to stop the compiler from reordering the stores and smp_wmb() to make the parameter words globally visible before the Pending bit is set.

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/6da466502621381fa88a6684290923d25c559266	Additional reference	git.kernel.org/stable/c/b3d346838ec65fac7fd83f5dbcedd13cadfffddb
Additional reference	git.kernel.org/stable/c/d6de766d8d26d71b714f548192099112def50a9c	NVD	nvd.nist.gov/vuln/detail/CVE-2026-98639
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103553	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98639

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