

CVE-2026-98390

Microsoft x86/amd_node: Avoid divide by zero on virtualized systems

In the Linux kernel, the following vulnerability has been resolved: x86/amd_node: Avoid divide by zero on virtualized systems
On a virtualized system, the number of nodes does not have a relationship to the number of roots. A Xen PVH dom0 can calculate roots_per_node as 0, which crashes with a divide by zero in: if (count++ % roots_per_node) because the underlying topology code on Xen ends up making num_nodes 2 and num_roots 1 and the integer division result is 0.

EVRS 0 /100 Informational priority	CVSS — Not scored	EPSS 0.002 10.1st 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)

The issue is seen with Xen, but it could affect other systems. Set roots_per_node to 1 in this case. Print a firmware bug when this is performed for non-virtualized systems. [bp: Massage commit message.]

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/72bd92bd8190d7869ecb462649ca40f297822a33	Additional reference	git.kernel.org/stable/c/9273a90465d58b82aca4bea71451ef6bee084928
Additional reference	git.kernel.org/stable/c/94e984d8858a3228952b02f84e66610961098cc2	NVD	nvd.nist.gov/vuln/detail/CVE-2026-98390
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-101039	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98390

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