

CVE-2026-98791

Microsoft net/mlx5e: Fix AF_XDP TX timestamp teardown NULL dereference

In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: Fix AF_XDP TX timestamp teardown NULL dereference During XSK TX queue teardown, outstanding descriptors are completed without a COE. If one requested a TX timestamp, the completion path passes that NULL COE to mlx5e_xsk_fill_timestamp(), which dereferences it. Return zero when no COE is available, indicating that teardown did not produce a TX timestamp.

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 KEY	Not currently CISA KEY-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 KEY 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/63df0ef4c6e3105589e6bb2e758ce611b0ada86c	Additional reference	git.kernel.org/stable/c/7b97273cbebe9dd4fddc457f0c4f2a124d0e3996
Additional reference	git.kernel.org/stable/c/f81d40e2eb69552334f510114f3e6edd0d43178b	Additional reference	git.kernel.org/stable/c/fce70b6bf9f3261e887419a4e7caa25b80fa9d55
NVD	nvd.nist.gov/vuln/detail/CVE-2026-98791	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103876
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98791		

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