

CVE-2026-98497

Microsoft net/mlx5e: fix swapped IPv6 IPsec policy masks

In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: fix swapped IPv6 IPsec policy masks IPv6 XFRM policies may use different source and destination prefix lengths. mlx5e_ipsec_policy_mask() builds the corresponding masks independently, but setup_fte_addr6() installs each mask in the opposite address field. When the prefix lengths differ, this makes the source match use the destination prefix and the destination match use the source prefix.

EVRS 0 /100 Informational priority	CVSS — Not scored	EPSS 0.002 9th 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 resulting hardware rule can both miss traffic covered by the policy and match traffic outside it. Install each mask in its corresponding match field.

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/10de7ed8ef4840da9ca21de4c29578657ac367db	Additional reference	git.kernel.org/stable/c/3803dc8477f08e0dac4050cafee0de43f32727be
Additional reference	git.kernel.org/stable/c/e73f832f0a7b2c6ea45b2124c732d639be97b547	NVD	nvd.nist.gov/vuln/detail/CVE-2026-98497
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103737	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98497

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