

CVE-2026-98618

Microsoft eth: fbnic: Handle maximum standalone channels

In the Linux kernel, the following vulnerability has been resolved: eth: fbnic: Handle maximum standalone channels Standalone channels use one NAPI vector for each Tx and Rx queue. fbnic's allocation path excludes FBNIC_MAX_TXQS from that layout. A 64-Tx/64-Rx configuration therefore records 128 vectors but allocates only 64, leaving NULL entries that resource setup dereferences. Include the maximum vector count in standalone allocation.

EVRS 0 /100 Informational priority	CVSS — Not scored	EPSS 0.002 9.2nd 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)

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/16ff1023213cc39c1a7ce737205c2a1a53c3a716	Additional reference	git.kernel.org/stable/c/1f4c73064a50f53d596c6f1d06d2d700f43c4b32
Additional reference	git.kernel.org/stable/c/6c903188b67617070017305a325fa326f270a43d	Additional reference	git.kernel.org/stable/c/9843e5fabd6ab296df9c025b1d0e5bf79a6b8a08
NVD	nvd.nist.gov/vuln/detail/CVE-2026-98618	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103663
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98618		

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