

CVE-2026-98277

Microsoft eth: fbnic: ring the doorbell if a burst ends in a drop

In the Linux kernel, the following vulnerability has been resolved: eth: fbnic: ring the doorbell if a burst ends in a drop
fbnic_tx_map() skips the doorbell write, and the completion request, for every packet handed to it with xmit_more set, counting on the packet which ends the burst to publish them all. When that packet is dropped instead - skb_put_padto(), skb_cow_head() or a DMA mapping failure - nothing rings.

EVRS 0 /100 Informational priority	CVSS — Not scored	EPSS 0.002 7.8th 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 descriptors of the preceding packets stay invisible to the HW until the next transmit on that queue, which for a burst-then-idle workload may never come. Remember the meta descriptor of the last packet left without a doorbell and flush it from the error paths. The completion request has to be set on that descriptor rather than simply writing the tail, otherwise the HW would transmit the packets but never report a head, and the ring would fill up and stall for good. This is very similar to Joe's recent series of fixes for bnxt. Not seen in real life, reproduced under QEMU with failure injection.

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/28fb764d670aa22dcbd2a02fd8fd87ae8d3563a9	Additional reference	git.kernel.org/stable/c/490599ab23134962a6d18a024e84541d77bdb999
Additional reference	git.kernel.org/stable/c/60ef74357a36ed2a102a75bb68d37aa7f305b94e	NVD	nvd.nist.gov/vuln/detail/CVE-2026-98277
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-93205	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98277

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