

CVE-2026-98615

Microsoft eth: fbnic: Set AW_FLUSH_MODE alongside AW_FLUSH when flushing the mailbox

In the Linux kernel, the following vulnerability has been resolved: eth: fbnic: Set AW_FLUSH_MODE alongside AW_FLUSH when flushing the mailbox When tearing down the FW mailbox Rx ring, fbnic_mbx_reset_desc_ring() writes AW_CFG with FLUSH set and everything else, BME included, cleared. Clearing BME halts the device's writes to the host but leaves the staged requests parked in the PUL write pipeline rather than draining them, so on the write path FLUSH alone never terminates the outstanding requests and the flush the

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 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)

firmware waits on never completes. Add the FLUSH_MODE definition and set both bits so the staged writes drain out of the pipeline on their own. BME stays cleared, so nothing lands on the host; it is restored later in fbnic_mbx_init_desc_ring() when the ring is rebuilt, once the outstanding writes are gone. The read path is unaffected. AR_CFG has no equivalent mode bit and AR_FLUSH terminates the outstanding reads by itself, so it is left as is. Both writes remain plain stores rather than read-modify-writes. That is deliberate: the matching write in fbnic_mbx_init_desc_ring() restores BME and the TLP attributes, and clears both flush bits as a side effect.

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/8947f13e436a4ff5eed9f8f019b2865a07af4bb2	Additional reference	git.kernel.org/stable/c/8a052cd4b2caee1f90cf0e3874377066939c90e7
Additional reference	git.kernel.org/stable/c/a969db6548a1b046cd1423701f5f9c3f5794e90d	Additional reference	git.kernel.org/stable/c/ed4163f6ba9b52bfd6216d5215ee7b8eb5072411
NVD	nvd.nist.gov/vuln/detail/CVE-2026-98615	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103660
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98615		

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