

CVE-2026-98375

Microsoft xen/netfront: drop RX packets with a short Ethernet header

In the Linux kernel, the following vulnerability has been resolved: xen/netfront: drop RX packets with a short Ethernet header
handle_incoming_queue() pulls pull_to bytes into the head before calling eth_type_trans(). pull_to is the length of the first RX slot, capped at RX_COPY_THRESHOLD, and that length comes from the backend. Nothing checks it against ETH_HLEN.

EVRS 0 /100 Informational priority	CVSS — Not scored	EPSS 0.002 6.8th 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)

If the first slot is shorter than ETH_HLEN and more slots follow, the head ends up shorter than an Ethernet header while skb->len is longer, and eth_type_trans() BUG()s in __skb_pull(). If the whole packet is shorter than ETH_HLEN, eth_type_trans() reads the header past the end of the data instead. Pull at least ETH_HLEN, and drop the packet if that fails, which also drops packets too short to hold an Ethernet header. This also checks the return value of the pull, which was ignored.

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/089e58805c452e52179482b1025a8e309a57f801	Additional reference	git.kernel.org/stable/c/236a17caebcff31f75bec5ff4136bde2de944e40
Additional reference	git.kernel.org/stable/c/72d2f54367895d6e236b9857892e2e6b6036e067	Additional reference	git.kernel.org/stable/c/e2b721bc30f40ffa7ccc36a56d4e8990b8c0538e
NVD	nvd.nist.gov/vuln/detail/CVE-2026-98375	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-95525
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98375		

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