

CVE-2026-98571

Microsoft net: stmmac: clear stale buf->page after recycling on skb build failure

In the Linux kernel, the following vulnerability has been resolved: net: stmmac: clear stale buf->page after recycling on skb build failure In stmmac_rx(), when napi_build_skb() fails the descriptor page is recycled back to the page pool with page_pool_recycle_direct(), but buf->page is left pointing at the recycled page, unlike every other consumption site in the function which clears the pointer after handing the page away.

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)

With the stale pointer stmmac_rx_refill() skips the replacement allocation and programs the already-recycled page back into the RX descriptor. Clear buf->page on the napi_build_skb() failure path to keep the buffer lifecycle consistent with the other consumption sites.

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/0a7822e34a0bfde31b194ac3da3253e5032b44cc	Additional reference	git.kernel.org/stable/c/298673397ea3f6f5811b84f0d9f71eac71dda2e3
Additional reference	git.kernel.org/stable/c/501baaeca7d128fa0a2f6953cf5873c5b0d7cf89	NVD	nvd.nist.gov/vuln/detail/CVE-2026-98571
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103616	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98571

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