

CVE-2026-98574

Microsoft net: bcmgenet: stop Tx NAPI before disabling the queues

In the Linux kernel, the following vulnerability has been resolved: net: bcmgenet: stop Tx NAPI before disabling the queues
bcmgenet_netif_stop() and the Wake-on-LAN branch of bcmgenet_suspend() both disable the Tx queues first and stop Tx NAPI several steps later. A completion in flight calls netif_tx_wake_queue() in between, and nothing stops the queue again, so a transmit can reach the rings after they have been freed. Close is safe because dev_deactivate_many() stops the qdisc first.

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)

bcmgenet_suspend() does not, so stop Tx NAPI before the queues on both paths. KASAN on a Raspberry Pi CM4, driven from an MTU change because suspend freezes user space before the callback runs: BUG: KASAN: use-after-free in bcmgenet_xmit+0x17f8/0x2258 Write of size 8 at addr ffffff8055844a68 by task ksoftirqd/0/14
bcmgenet_xmit+0x17f8/0x2258 dev_hard_start_xmit+0x13c/0x588 sch_direct_xmit+0x108/0x340
__dev_queue_xmit+0x1190/0x3848

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/63bcc2fee6419963e45e7c2cd698fa862409601d	Additional reference	git.kernel.org/stable/c/7e87508b5c4d81210d0a736ed01962e52f5c4c56
Additional reference	git.kernel.org/stable/c/f329d42423089904758f2685cda295de9bf99441	NVD	nvd.nist.gov/vuln/detail/CVE-2026-98574
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103619	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98574

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