

CVE-2026-98693

Microsoft thunderbolt: Hold a router reference for each allocated HopID

In the Linux kernel, the following vulnerability has been resolved: thunderbolt: Hold a router reference for each allocated HopID
tb_stop() drops the reference to all DP tunnels but does not deactivate them, thus nothing cancels a dprx_work still in flight (which holds its own tunnel reference) and the tunnel can outlive tb_switch_remove(). The HopID releases in tb_path_free() then operate on freed IDAs and trigger warnings like ida_free called for id=8 which is not allocated.

EVRS	CVSS	EPSS	CISA DEADLINE
0/100	—	0.002	—
Informational priority	Not scored	9th percentile · FIRST	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)

This can be triggered by unbinding the driver while a DP tunnel is still waiting for the DPRX capabilities read to finish. On the Apple NHI unplugging the cable runs into just that reliably because the read can never finish right now and because the unplug powers down the entire USB4 complex and removes the NHI device. Take a router reference whenever an input or output HopID is allocated and drop it again after the HopID is released. This keeps the ports and their HopID IDAs alive for as long as they are used. The KUnit tests allocate routers without ever registering their devices so initialize the embedded struct device there as well and drop its initial reference when the test is finished.

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/032c59c7681c661b63123231824170c025afb7e7	Additional reference	git.kernel.org/stable/c/2b5f976119d8f099a03cbf700df3d9c8690fe33d
Additional reference	git.kernel.org/stable/c/c444d2c17dc236680324fd989232199680a6c419	NVD	nvd.nist.gov/vuln/detail/CVE-2026-98693
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103947	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98693

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