

CVE-2026-98691

Microsoft thunderbolt: Tear down inactive DP tunnels when the domain is stopped

In the Linux kernel, the following vulnerability has been resolved: thunderbolt: Tear down inactive DP tunnels when the domain is stopped tb_stop() only tears down DMA tunnels so a DP tunnel that is still waiting for dprx_work to complete keeps that work queued while the routers are removed and the control channel is stopped. The work only stops once the DPRX timeout has passed and because it requeues itself until then the flush_workqueue() in tb_domain_remove() won't wait for its final run.

EVRS 0 /100 Informational priority	CVSS — Not scored	EPSS 0.002 5.5th 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)

The callback then runs against a domain that is already torn down. A reference to that domain is kept so the completion waiting for that domain to disappear in unbind will block until the timeout is eventually reached. Tear down DP tunnels that are not active yet as well which also cancels that work. Tunnels for displays that are already alive are untouched and keep working.

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/0b457c6733f73421a3fb03786f13d67c618b5119	Additional reference	git.kernel.org/stable/c/34a6e27c954e5bfc29fead17867c7155d54b6481
Additional reference	git.kernel.org/stable/c/cbd2abb85ea32cafdcbaba218e13b18d8ed79bfa	NVD	nvd.nist.gov/vuln/detail/CVE-2026-98691
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103945	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98691

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