

CVE-2026-98690

Microsoft thunderbolt: Fix domain reference leak when DPRX read is canceled

In the Linux kernel, the following vulnerability has been resolved: thunderbolt: Fix domain reference leak when DPRX read is canceled tb_tunnel_one_dp() takes a domain reference which is only dropped once tb_dp_tunnel_active() has run on the work queue. If that work is cancelled that reference is leaked. Since commit f5cc545f5969 ("thunderbolt: Wait for tb_domain_release() to complete when driver is removed") instead of just leaking memory this now also blocks in the completion wait forever when unbinding the

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)

driver. This can be triggered whenever a DP tunnel is torn down before the DPRX read has completed, e.g. by unplugging within the timeout, and then unbinding the driver. That reference only exists to keep the domain around while the DPRX work is scheduled so let the work itself own it: take it in tb_dp_dprx_start() and drop it in both places that end the work. Get/put are then paired inside the same file and it doesn't matter anymore if the callback ever runs.

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/1fd1f67c94d30889377bba774f032ec15e8b9299	Additional reference	git.kernel.org/stable/c/2f5893172fc6153f5f1ef34014ddbfcfbf1f47f29
Additional reference	git.kernel.org/stable/c/7739b02129b2248f9a8054cfda924fa253f66a88	NVD	nvd.nist.gov/vuln/detail/CVE-2026-98690
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103944	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98690

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