

CVE-2026-98692

Microsoft thunderbolt: Make the DP tunnel activation callback mandatory

In the Linux kernel, the following vulnerability has been resolved: thunderbolt: Make the DP tunnel activation callback mandatory `tb_tunnel_alloc_dp()` takes an optional callback which is run from `dprx_work` once the DPRX capabilities read has completed. Without that callback `tb_dp_dprx_start()` reads the capabilities synchronously and never queues the work.

EVRS 0 /100 Informational priority	CVSS — Not scored	EPSS 0.002 4.3rd 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)

It however always takes a tunnel reference which is only dropped by `dprx_work` itself or by `tb_dp_dprx_stop()` when `cancel_delayed_work()` actually canceled that work. That reference is thus leaked for every tunnel without a callback. The only tunnels without one are those from `tb_tunnel_discover_dp()`, which are activated again when restoring from hibernation. Pass the callback to `tb_tunnel_discover_dp()` as well and drop the synchronous path such that the DPRX capabilities are always read from `dprx_work`. Hibernation restore then also no longer blocks for up to 12 seconds while waiting for that read to complete. Also fix up the KUnit tests.

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/12f5d8b85a66a0ac08d082517d92ce136f8c0d42

NVD nvd.nist.gov/vuln/detail/CVE-2026-98692

Current data evulnable.com/vulnerability-management/cve/CVE-2026-98692

Additional reference git.kernel.org/stable/c/47d60ea801fc333a10c576691eca2e7840b02d3d

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2026-103946

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