

CVE-2026-98689

Microsoft thunderbolt: Don't access a DP tunnel after its DPRX read was canceled

In the Linux kernel, the following vulnerability has been resolved: thunderbolt: Don't access a DP tunnel after its DPRX read was canceled `tb_dp_dprx_work()` checks `->dprx_canceled` before it takes `tb->lock` so it misses a `tb_dp_dprx_stop()` that could not cancel the already running work. It then polls the DPRX capabilities and runs the callback for a tunnel that has already been torn down while the domain is suspending or going away.

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)

This can be hit by cancelling the DPRX read from outside the ordered `tb->wq`: During suspend `tb_disconnect_and_release_dp()` does just this and with a later patch `tb_stop()` will do it as well. The latter in combination with the Apple NHI where the DPRX read never completed is how I hit this. Check the flag with `tb->lock` held instead and check it again in `tb_dp_tunnel_active()` because the callback runs after the lock has been dropped again. Also clear the flag in `tb_dp_dprx_start()` so that it only ever describes the work that is currently in flight.

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/2c2fd6a7fd5e1218db7e17336fc1a0393b6949e6	Additional reference	git.kernel.org/stable/c/405a969c0b3356639116db89ab367be1d64b77c0
Additional reference	git.kernel.org/stable/c/419fa32fa5bc2d7fb9d0d15d5630b1c1090808b3	NVD	nvd.nist.gov/vuln/detail/CVE-2026-98689
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103943	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98689

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