

CVE-2026-98759

Microsoft usb: typec: tipd: fix uninitialized typec_partner_desc in cd321x_update_work()

In the Linux kernel, the following vulnerability has been resolved: usb: typec: tipd: fix uninitialized typec_partner_desc in cd321x_update_work() cd321x_update_work() passes a stack-allocated typec_partner_desc to typec_register_partner() after initializing only usb_pd, accessory and identity. typec_register_partner() copies attach and detach from the descriptor into the partner.

EVRS 0 /100 Informational priority	CVSS — Not scored	EPSS 0.002 10.1st 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)

With those fields left unset, garbage function pointers may be stored and later invoked from typec_partner_link_device() when a USB device is linked to the port. Uninitialized pd_revision and usb_capability similarly leak stack data through partner sysfs. Zero-initialize the descriptor so optional callbacks remain NULL and the remaining fields are zero.

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/5414144e202a32437e3eb436cd3f5f00d79ad86e	Additional reference	git.kernel.org/stable/c/75dc6cb377efd2f4428b7f76d3a590a0bbc10399
Additional reference	git.kernel.org/stable/c/88c7e458af53ff781a3f1051708395892b325576	NVD	nvd.nist.gov/vuln/detail/CVE-2026-98759
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103844	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98759

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