

CVE-2026-98849

Microsoft pfcpl: fix socket lifetime on netdevice registration failure

In the Linux kernel, the following vulnerability has been resolved: pfcpl: fix socket lifetime on netdevice registration failure
pfcpl_newlink() creates the UDP socket before register_netdevice(). If registration fails after pfcpl_dev_init() succeeds, the core calls pfcpl_dev_uninit(), which releases the socket and clears pfcpl->sk. The newlink error path then releases it again, causing a NULL pointer dereference. This was observed with failslab fault injection: FAULT_INJECTION: forcing a failure.

EVRS 0 /100 Informational priority	CVSS — Not scored	EPSS 0.002 5.8th 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)

kobject: kobject_add_internal failed for pfcpl0 (error: -12 parent: net) BUG: KASAN: null-ptr-deref in udp_tunnel_sock_release+0x1c/0x50 Read of size 8 at addr 0000000000000120 by task ip/1037 Call trace: show_stack+0x18/0x24 (C) dump_stack_lvl+0x78/0x90 print_report+0x468/0x5cc kasan_report+0xa4/0xf0 __asan_load8+0x7c/0xd0 udp_tunnel_sock_release+0x1c/0x50 pfcpl_newlink+0x128/0x184 rtnl_newlink+0x848/0xe44 rtnetlink_rcv_msg+0x468/0x514 netlink_rcv_skb+0xc0/0x1f0 rtnetlink_rcv+0x18/0x24 netlink_unicast+0x4b8/0x558 netlink_sendmsg+0x2b8/0x584 ... Return from pfcpl_del_sock() if pfcpl->sk is NULL.

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/0f17d2e3dd9cda3ee6d94033d5e5489af168920d	Additional reference	git.kernel.org/stable/c/2cee3603ec1d9b5ec7f2121ea3efe9488e906f46
Additional reference	git.kernel.org/stable/c/4b8ce1686dea1a10805a0807bf492409b0300ee1	Additional reference	git.kernel.org/stable/c/dcb8f6a79c3360a440c399d85df465a6e59351f1
NVD	nvd.nist.gov/vuln/detail/CVE-2026-98849	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103789
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98849		

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