

CVE-2026-98240

Microsoft net: ip_tunnel: initialize `options\_len` before referencing options

In the Linux kernel, the following vulnerability has been resolved: net: ip_tunnel: initialize `options\_len` before referencing options The following command triggers a kernel panic: ip link add d0 type dummy; ip link set d0 up ip route add 10.30.0.0/16 \ encap ip id 300 geneve_opts 4660:66:11223344 dev d0 memcpy: detected buffer overflow: 4 byte write of buffer size 0 kernel BUG at lib/string_helpers.c:1044! ...

EVRS	CVSS	EPSS	CISA DEADLINE
0/100	—	0.002	—
Informational priority	Not scored	7.4th percentile · FIRST	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)

ip_tun_parse_opts.part.0.cold+0x10/0x10 ip_tun_build_state+0x116/0x2a0 On kernels built with GCC 15+ and `CONFIG\_FORTIFY\_SOURCE`, the fortified `memcpy()` got 0 sized destination with request of 4 bytes length: static int ip_tun_parse_opts_geneve(...) { ... attr = tb[LWTUNNEL_IP_OPT_GENEVE_DATA]; data_len = nla_len(attr); /* == 4 */ struct geneve_opt *opt = ip_tunnel_info_opts(info) + opts_len; memcpy(opt->opt_data, nla_data(attr), data_len); /* ^^^^^^^^^^^^^^ 0 since options_len is assigned afterwards */ Fixed by initializing the counter before the options are referenced. Matching what `tunnel\_key\_opts\_set()` already does.

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/0f6a6beb01c068fcd5274eabf22c260039749fea	Additional reference	git.kernel.org/stable/c/455ebeadf714f51e1dbbd6a022c74c9215b1cd76
Additional reference	git.kernel.org/stable/c/9907325257b4b382f26aafd5d9a8d47915907dd5	NVD	nvd.nist.gov/vuln/detail/CVE-2026-98240
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-93168	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98240

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