

CVE-2026-98596

Microsoft ipv6: Fix dst leak for uncached routes.

In the Linux kernel, the following vulnerability has been resolved: ipv6: Fix dst leak for uncached routes. ip6_route_output_flags(), ip6_rt_put_flags(), and ip6_dst_check() detect an uncached route by list_empty(&rt->dst.rt_uncached), which replaced the static DST_NOCACHE flag check in commit a4c2fd7f7891 ("net: remove DST_NOCACHE flag"). When a device is unregistered, rt6_uncached_list_flush_dev() unlinks uncached routes tied to the device from rt6_uncached_list.

EVRS	CVSS	EPSS	CISA DEADLINE
0/100 Informational priority	— Not scored	0.002 9.3rd 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)

Previously, they were moved to another list with list_move() (__list_del_entry() + list_add()), and since commit 98aa546af5e4 ("inet: remove (struct uncached_list)->quarantine"), the routes are just unlinked with list_del_init(). If list_del_init() runs concurrently, list_empty() evaluates to true; ip6_route_output_flags() calls dst_hold_safe() incorrectly and ip6_rt_put_flags() skips ip6_rt_put(), leaking dst, and thus dev tied via rt->from as well. The same race is partially fixed by commit 9a6f0c4d5796 ("dst: fix races in rt6_uncached_list_del() and rt_del_uncached_list()"). Let's check rt6->dst.rt_uncached_list instead. Note that IPv4 does not have the same issue.

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/5045aa25f3790dcdcb158a58ac60ccf8da42959aa	Additional reference	git.kernel.org/stable/c/be31fe6333f534155e6b408f1ef6d77974bb41aa
Additional reference	git.kernel.org/stable/c/ed902d5546fb9c142b3216d8eec914fa1bc0aa80	Additional reference	git.kernel.org/stable/c/f9722746df13a8a29103c847ef56b02c11ce0963
NVD	nvd.nist.gov/vuln/detail/CVE-2026-98596	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103641
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98596		

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