

CVE-2026-98603

Microsoft ovpn: replace bind when clearing stale local source

In the Linux kernel, the following vulnerability has been resolved: ovpn: replace bind when clearing stale local source The UDP output fallback clears bind->local in place when the remembered source address is no longer usable. The bind is RCU-published and read locklessly by concurrent TX, so an IPv6 reader can observe a torn address. Retry the route lookup with source address autoselection without modifying the bind.

EVRS 0 /100 Informational priority	CVSS — Not scored	EPSS 0.002 9th 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)

After a successful lookup, revalidate the bind and route key under peer->lock, reset the dst cache, and best-effort publish a replacement bind with a wildcard local address. Do not cache the resolved dst when clearing the local source. Replacing the source invalidates all per-CPU cache entries, while dst_cache_set_ip4 and dst_cache_set_ip6 update only the current CPU slot. The current packet can still use the resolved route; if bind allocation fails, a later cache miss retries the repair.

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/72bd1bea37ea2c8553938f086bf48ccd2147dfe1	Additional reference	git.kernel.org/stable/c/7d8104988f423572df1f3347ce578037b1043f34
Additional reference	git.kernel.org/stable/c/c44a04722f7dae9a45a101b8e100931ab59f1c18	NVD	nvd.nist.gov/vuln/detail/CVE-2026-98603
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103648	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98603

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