

# CVE-2026-98487

## Microsoft net: bridge: mdb: restart port group walk after deletion

In the Linux kernel, the following vulnerability has been resolved: net: bridge: mdb: restart port group walk after deletion  
br\_mdb\_flush\_pgs() keeps a pointer-to-pointer cursor while walking mp->ports. br\_multicast\_del\_pg() can re-enter the same MDB entry through br\_multicast\_sg\_del\_exclude\_ports() and unlink other port groups. If the cursor points into one of those groups, the next iteration dereferences a stale cursor and can leave mp->ports pointing at freed memory.

|                                                 |                         |                                                  |                                        |
|-------------------------------------------------|-------------------------|--------------------------------------------------|----------------------------------------|
| EVRS<br><b>0</b> /100<br>Informational priority | CVSS<br>—<br>Not scored | EPSS<br><b>0.002</b><br>9.3rd percentile · FIRST | CISA DEADLINE<br>—<br>No CISA deadline |
|-------------------------------------------------|-------------------------|--------------------------------------------------|----------------------------------------|

## Signals behind the score

☒ counted in the score ☐ not counted

evidence for 2 of 8 signals

|                                            |                                    |                                                                |                                                                                                    |
|--------------------------------------------|------------------------------------|----------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> <b>CISA KEV</b>   | Not currently CISA KEV-listed      | <input type="checkbox"/> <b>Vendor exploitation</b>            | Active-exploitation status not yet checked - scored at the population base rate (none) until known |
| <input type="checkbox"/> <b>Ransomware</b> | Ransomware association unavailable | <input type="checkbox"/> <b>KEV recency</b>                    | CISA KEV listing date unavailable                                                                  |
| <input type="checkbox"/> <b>EPSS</b>       | 0.002 probability                  | <input type="checkbox"/> <b>Pre-patch disclosure</b>           | Disclosure status unavailable                                                                      |
| <input type="checkbox"/> <b>CVSS</b>       | CVSS base score unavailable        | <input type="checkbox"/> <b>Microsoft Exploitability Index</b> | 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)

A following RTM\_GETMDB exposes the dangling pointer: BUG: KASAN: slab-use-after-free in br\_mdb\_dump Read of size 8  
br\_mdb\_dump rtnl\_mdb\_dump rtnl\_dumpit netlink\_dump Reset the cursor to mp->ports after every deletion. The deletion removes at least the selected group, so the restarted walk always makes progress.

## Affected and fixed versions

| PACKAGE                                 | AFFECTED | FIXED IN                | SOURCE |
|-----------------------------------------|----------|-------------------------|--------|
| Not identified by the connected sources | —        | no fixed version listed | NVD    |

## Sources

|                      |                                                                                                                                                         |                      |                                                                                                                                                         |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| Reference            | <a href="https://git.kernel.org/stable/c/46ec55855c972504258c371677ac039ba20e5d12">git.kernel.org/stable/c/46ec55855c972504258c371677ac039ba20e5d12</a> | Additional reference | <a href="https://git.kernel.org/stable/c/ab1404ac81154a89fb61ac50ae9a04cd8d4834dc">git.kernel.org/stable/c/ab1404ac81154a89fb61ac50ae9a04cd8d4834dc</a> |
| Additional reference | <a href="https://git.kernel.org/stable/c/ab3c4a4c85f2e1e8d04b5c1770dea8412d21c7fe">git.kernel.org/stable/c/ab3c4a4c85f2e1e8d04b5c1770dea8412d21c7fe</a> | Additional reference | <a href="https://git.kernel.org/stable/c/fe2a42789c12eb7c5d3a42191e2cc735a6c35ead">git.kernel.org/stable/c/fe2a42789c12eb7c5d3a42191e2cc735a6c35ead</a> |
| NVD                  | <a href="https://nvd.nist.gov/vuln/detail/CVE-2026-98487">nvd.nist.gov/vuln/detail/CVE-2026-98487</a>                                                   | ENISA EUVD           | <a href="https://euvd.enisa.europa.eu/vulnerability/EUVD-2026-103727">euvd.enisa.europa.eu/vulnerability/EUVD-2026-103727</a>                           |
| Current data         | <a href="https://evulnable.com/vulnerability-management/cve/CVE-2026-98487">evulnable.com/vulnerability-management/cve/CVE-2026-98487</a>               |                      |                                                                                                                                                         |

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