



# netfilter: ctnetlink: use netlink policy range checks

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2026-31495                               |
| <b>State</b>           | PUBLISHED                                    |
| <b>Assigner</b>        | Linux  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback |
| <b>Published</b>       | 2026-04-22 14:16:47 UTC                      |
| <b>Updated</b>         | 2026-04-22 14:16:47 UTC                      |

**Description** In the Linux kernel, the following vulnerability has been resolved: netfilter: ctnetlink: use netlink policy range checks Replace

## Vendor Declared Affected Products

| Source | Vendor                | Product               | Version  |
|--------|-----------------------|-----------------------|--|
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | affected c8e2078cfe414a99cf6f2f2f1d78c7e75392e9d4 435b576cd2faa75154777868f8cbb73bf71644d3 git |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | affected c8e2078cfe414a99cf6f2f2f1d78c7e75392e9d4 2ef71307c86a9f866d6e28f1a0c06e2e9d794474 git |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | affected c8e2078cfe414a99cf6f2f2f1d78c7e75392e9d4 4f7d25f3f0786402ba48ff7d13b6241d77d975f5 git |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | affected c8e2078cfe414a99cf6f2f2f1d78c7e75392e9d4 fcec5ce2d73a41668b24e3f18c803541602a59f6 git |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | affected c8e2078cfe414a99cf6f2f2f1d78c7e75392e9d4 675c913b940488a84effdeec5a1cfb657b59804 git  |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | affected c8e2078cfe414a99cf6f2f2f1d78c7e75392e9d4 c6cb41eaae875501eaaa487b8db6539feb092292 git |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | affected c8e2078cfe414a99cf6f2f2f1d78c7e75392e9d4 45c33e79ae705b7af97e3117672b6cd258dd0b1b git |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | affected c8e2078cfe414a99cf6f2f2f1d78c7e75392e9d4 8f15b5071b4548b0aafc03b366eb45c9c6566704 git |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | affected 2.6.22  |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | unaffected 2.6.22 semver   |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | unaffected 5.10.253 5.10.* semver  |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | unaffected 5.15.203 5.15.* semver  |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | unaffected 6.1.168 6.1.* semver  |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | unaffected 6.6.131 6.6.* semver  |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | unaffected 6.12.80 6.12.* semver   |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | unaffected 6.18.21 6.18.* semver   |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | unaffected 6.19.11 6.19.* semver   |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | unaffected 7.0 * original_commit_for_fix   |

## References

| Reference   | Source                               | Link  | Tags    |
|---|--------------------------------------|---|---------|
| <a href="https://git.kernel.org/stable/c/4f7d25f3f0786402ba48ff7d13b6241d77d975f5">git.kernel.org/stable/c/4f7d25f3f0786402ba48ff7d13b6241d77d975f5</a> | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org">git.kernel.org</a> |         |
| <a href="https://git.kernel.org/stable/c/c6cb41eaae875501eaaa487b8db6539feb092292">git.kernel.org/stable/c/c6cb41eaae875501eaaa487b8db6539feb092292</a> | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org">git.kernel.org</a> |         |
| <a href="https://git.kernel.org/stable/c/675c913b940488a84effdeeac5a1cfb657b59804">git.kernel.org/stable/c/675c913b940488a84effdeeac5a1cfb657b59804</a> | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org">git.kernel.org</a> |         |
| <a href="https://git.kernel.org/stable/c/fcec5ce2d73a41668b24e3f18c803541602a59f6">git.kernel.org/stable/c/fcec5ce2d73a41668b24e3f18c803541602a59f6</a> | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org">git.kernel.org</a> |         |
| <a href="https://git.kernel.org/stable/c/2ef71307c86a9f866d6e28f1a0c06e2e9d794474">git.kernel.org/stable/c/2ef71307c86a9f866d6e28f1a0c06e2e9d794474</a> | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org">git.kernel.org</a> |         |
| <a href="https://git.kernel.org/stable/c/45c33e79ae705b7af97e3117672b6cd258dd0b1b">git.kernel.org/stable/c/45c33e79ae705b7af97e3117672b6cd258dd0b1b</a> | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org">git.kernel.org</a> |         |
| <a href="https://git.kernel.org/stable/c/435b576cd2faa75154777868f8cbb73bf71644d3">git.kernel.org/stable/c/435b576cd2faa75154777868f8cbb73bf71644d3</a> | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org">git.kernel.org</a> |         |
| <a href="https://git.kernel.org/stable/c/8f15b5071b4548b0aa03b366eb45c9c6566704">git.kernel.org/stable/c/8f15b5071b4548b0aa03b366eb45c9c6566704</a>     | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org">git.kernel.org</a> |         |
| CVE Program record  | CVE.ORG                              | <a href="https://www.cve.org">www.cve.org</a>       | canonic |
| NVD vulnerability detail  | NVD                                  | <a href="https://nvd.nist.gov">nvd.nist.gov</a>     | canonic |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)