



# bpf: Fix unsound scalar forking in maybe\_fork\_scalars() for BPF\_OR

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2026-31413                               |
| <b>State</b>           | PUBLISHED                                    |
| <b>Assigner</b>        | Linux  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback |
| <b>Published</b>       | 2026-04-12 06:16:20 UTC                      |
| <b>Updated</b>         | 2026-04-12 06:16:20 UTC                      |

**Description** In the Linux kernel, the following vulnerability has been resolved: bpf: Fix unsound scalar forking in maybe\_fork\_scalars() fo

## Vendor Declared Affected Products

| Source | Vendor                | Product               | Version  |
|--------|-----------------------|-----------------------|--|
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | affected dea9989a3f3961faede93752cd81eb5a9514d911 342aa1ee995ef5bbf876096dc3a5e51218d76fa4 git |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | affected 4c122e8ae14950cf6b59d208fc5160f7c601e746 58bd87d0e69204dbd739e4387a1edb0c4b1644e7 gi  |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | affected e52567173ba86dbff990595f5be60e2e83899372 d13281ae7ea8902b21d99d10a2c8caf0bdec0455 git |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | affected bffacdb80b93b7b5e96b26fad64cc490a6c7d6c7 c845894ebd6fb43226b3118d6b017942550910c5 git |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | affected 7.0-rc1   |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | unaffected 7.0-rc1 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-rc5 * original_commit_for_fix   |

## References

| Reference  | Source                               | Link                           | Tags    |
|--|--------------------------------------|--------------------------------|---------|
| git.kernel.org/stable/c/58bd87d0e69204dbd739e4387a1edb0c4b1644e7 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="#">git.kernel.org</a> |         |
| git.kernel.org/stable/c/c845894ebd6fb43226b3118d6b017942550910c5 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="#">git.kernel.org</a> |         |
| git.kernel.org/stable/c/342aa1ee995ef5bbf876096dc3a5e51218d76fa4 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="#">git.kernel.org</a> |         |
| git.kernel.org/stable/c/d13281ae7ea8902b21d99d10a2c8caf0bdec0455 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="#">git.kernel.org</a> |         |
| CVE Program record   | CVE.ORG                              | <a href="#">www.cve.org</a>    | canonic |
| NVD vulnerability detail   | NVD                                  | <a href="#">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](#) 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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

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

**CVE.report and Source URL Uptime Status** [status.cve.report](#)