



# net: fix fanout UAF in packet\_release() via NETDEV\_UP race

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

## Summary

<b>CVE</b>	CVE-2026-31504
<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 14:16:49 UTC
<b>Updated</b>	2026-04-22 14:16:49 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: net: fix fanout UAF in packet\_release() via NETDEV\_UP r

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected ce06b03e60fc19c680d1bf873e779bf11c2fc518 ee642b1962caa9aa231c01abbd58bc453ae6b66e git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected ce06b03e60fc19c680d1bf873e779bf11c2fc518 42cfd7898eed290c9fb73f732af1f7d6b0a703e git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected ce06b03e60fc19c680d1bf873e779bf11c2fc518 1b4c03f8892d955385c202009af7485364731bb9 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected ce06b03e60fc19c680d1bf873e779bf11c2fc518 654386baef228c2992dbf604c819e4c7c35fc71b git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected ce06b03e60fc19c680d1bf873e779bf11c2fc518 75fe6db23705a1d55160081f7b37db9665b1880b git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected ce06b03e60fc19c680d1bf873e779bf11c2fc518 d0c7cdc15fdf8c4f91aca1928e52295d175b6ec6 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected ce06b03e60fc19c680d1bf873e779bf11c2fc518 ceccbfc6de720ad633519a226715989cfb065af1 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected ce06b03e60fc19c680d1bf873e779bf11c2fc518 42156f93d123436f2a27c468f18c966b7e5db796 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 3.1
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 3.1 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/42cfd7898eeed290c9fb73f732af1f7d6b0a703e">git.kernel.org/stable/c/42cfd7898eeed290c9fb73f732af1f7d6b0a703e</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/ee642b1962caa9aa231c01abbd58bc453ae6b66e">git.kernel.org/stable/c/ee642b1962caa9aa231c01abbd58bc453ae6b66e</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/1b4c03f8892d955385c202009af7485364731bb9">git.kernel.org/stable/c/1b4c03f8892d955385c202009af7485364731bb9</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/75fe6db23705a1d55160081f7b37db9665b1880b">git.kernel.org/stable/c/75fe6db23705a1d55160081f7b37db9665b1880b</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/ceccbfc6de720ad633519a226715989cfb065af1">git.kernel.org/stable/c/ceccbfc6de720ad633519a226715989cfb065af1</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/d0c7cdc15fdf8c4f91aca1928e52295d175b6ec6">git.kernel.org/stable/c/d0c7cdc15fdf8c4f91aca1928e52295d175b6ec6</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/654386baef228c2992dbf604c819e4c7c35fc71b">git.kernel.org/stable/c/654386baef228c2992dbf604c819e4c7c35fc71b</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/42156f93d123436f2a27c468f18c966b7e5db796">git.kernel.org/stable/c/42156f93d123436f2a27c468f18c966b7e5db796</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://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/licenses).

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)