



# team: fix header\_ops type confusion with non-Ethernet ports

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

## Summary

<b>CVE</b>	CVE-2026-31502
<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 14:16:48 UTC
<b>Updated</b>	2026-04-22 14:16:48 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: team: fix header\_ops type confusion with non-Ethernet po

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 1d76efe1577b4323609b1bcbfafa8b731eda071a 6d3161fa3eee64d46b766fb0db33ec7f300ef52d git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 1d76efe1577b4323609b1bcbfafa8b731eda071a 0a7468ed49a6b65d34abcc6eb60e15f7f6d34da0 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 1d76efe1577b4323609b1bcbfafa8b731eda071a 20491d384d973a63fbdaf7a71e38d69b0659ea55 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 1d76efe1577b4323609b1bcbfafa8b731eda071a 425000dbf17373a4ab8be9428f5dc055ef870a56 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 3.7
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 3.7 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
git.kernel.org/stable/c/425000dbf17373a4ab8be9428f5dc055ef870a56	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="#">git.kernel.org</a>	
git.kernel.org/stable/c/6d3161fa3eee64d46b766fb0db33ec7f300ef52d	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="#">git.kernel.org</a>	
git.kernel.org/stable/c/0a7468ed49a6b65d34abcc6eb60e15f7f6d34da0	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="#">git.kernel.org</a>	
git.kernel.org/stable/c/20491d384d973a63fbdaf7a71e38d69b0659ea55	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="#">git.kernel.org</a>	
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canonical

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](#)