



# virtio\_net: Fix UAF on dst\_ops when IFF\_XMIT\_DST\_RELEASE is cleared and napi\_tx is false

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

## Summary

<b>CVE</b>	CVE-2026-31469
<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 14:16:43 UTC
<b>Updated</b>	2026-04-22 14:16:43 UTC
<b>Description</b>	In the Linux kernel, the following vulnerability has been resolved: virtio_net: Fix UAF on dst_ops when IFF_XMIT_DST_RELEASE is cleared and napi_tx is false

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected f2fc6a54585a1be6669613a31fbaba2ecbadcd36 be0e63f3b97bbaf453c542e8a15ba2a536e2ac01 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected f2fc6a54585a1be6669613a31fbaba2ecbadcd36 c1ec36cb3768574b916f20d2d7415fd14fa1bf12 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected f2fc6a54585a1be6669613a31fbaba2ecbadcd36 8a4790850e710fd6771e4d2112168ed1dd6c0e54 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected f2fc6a54585a1be6669613a31fbaba2ecbadcd36 fedd2e1630cac920844997227ccbe7b26a76375a git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected f2fc6a54585a1be6669613a31fbaba2ecbadcd36 f04733c4dc40c43899c3d1c97afbae5831a3770f git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected f2fc6a54585a1be6669613a31fbaba2ecbadcd36 9a18629f2525781f0f3dda7be72b204e4cf77d08 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected f2fc6a54585a1be6669613a31fbaba2ecbadcd36 63d45077b97bb0e0fe0c75931acbbca7a47af141 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected f2fc6a54585a1be6669613a31fbaba2ecbadcd36 ba8bda9a0896746053aa97ac6c3e08168729172c git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 2.6.26
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 2.6.26 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/63d45077b97bb0e0fe0c75931acbbca7a47af141">git.kernel.org/stable/c/63d45077b97bb0e0fe0c75931acbbca7a47af141</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>		
<a href="https://git.kernel.org/stable/c/f04733c4dc40c43899c3d1c97afbae5831a3770f">git.kernel.org/stable/c/f04733c4dc40c43899c3d1c97afbae5831a3770f</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>		
<a href="https://git.kernel.org/stable/c/9a18629f2525781f0f3dda7be72b204e4cf77d08">git.kernel.org/stable/c/9a18629f2525781f0f3dda7be72b204e4cf77d08</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>		
<a href="https://git.kernel.org/stable/c/fedd2e1630cac920844997227ccbe7b26a76375a">git.kernel.org/stable/c/fedd2e1630cac920844997227ccbe7b26a76375a</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>		
<a href="https://git.kernel.org/stable/c/8a4790850e710fd6771e4d2112168ed1dd6c0e54">git.kernel.org/stable/c/8a4790850e710fd6771e4d2112168ed1dd6c0e54</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>		
<a href="https://git.kernel.org/stable/c/be0e63f3b97bbaf453c542e8a15ba2a536e2ac01">git.kernel.org/stable/c/be0e63f3b97bbaf453c542e8a15ba2a536e2ac01</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>		
<a href="https://git.kernel.org/stable/c/c1ec36cb3768574b916f20d2d7415fd14fa1bf12">git.kernel.org/stable/c/c1ec36cb3768574b916f20d2d7415fd14fa1bf12</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>		
<a href="https://git.kernel.org/stable/c/ba8bda9a0896746053aa97ac6c3e08168729172c">git.kernel.org/stable/c/ba8bda9a0896746053aa97ac6c3e08168729172c</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/cve).

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)