



# netfilter: nfnetlink\_queue: fix entry leak in bridge verdict error path

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

## Summary

<b>CVE</b>	CVE-2026-43451
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-08 15:16:57 UTC
<b>Updated</b>	2026-05-08 15:16:57 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: netfilter: nfnetlink\_queue: fix entry leak in bridge verdict er

## Risk And Classification

**EPSS:** 0.000240000 probability, percentile 0.070210000 (date 2026-05-11)

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 8d45ff22f1b43249f0cf1baafe0262ca10d1666e a907bea273b60d3e604ec4e8e1f6c49954805794 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 8d45ff22f1b43249f0cf1baafe0262ca10d1666e 0b18d1b834ab5a5009be70b530f978d7989e445b git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 8d45ff22f1b43249f0cf1baafe0262ca10d1666e b38d2b4603fd3dda24eb8b3dd81c18a0930be97b git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 8d45ff22f1b43249f0cf1baafe0262ca10d1666e 47b1c5d1b0944aa88299f55a846fabaefc756982 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 8d45ff22f1b43249f0cf1baafe0262ca10d1666e cf4a4df38d1747e06fc54f9879bd7a6f4178032f git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 8d45ff22f1b43249f0cf1baafe0262ca10d1666e 9853d94b82d303fc4ac37d592a23a154096ecd41 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 8d45ff22f1b43249f0cf1baafe0262ca10d1666e 208669df703a25a601f45822b10c413f258bf275 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 8d45ff22f1b43249f0cf1baafe0262ca10d1666e f1ba83755d81c6fc66ac7acd723d238f974091e9 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 4.7
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 4.7 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 6.1.167 6.1.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.6.130 6.6.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.12.78 6.12.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.18.19 6.18.* semver

CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.19.9 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/9853d94b82d303fc4ac37d592a23a154096ecd41">git.kernel.org/stable/c/9853d94b82d303fc4ac37d592a23a154096ecd41</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/cf4a4df38d1747e06fc54f9879bd7a6f4178032f">git.kernel.org/stable/c/cf4a4df38d1747e06fc54f9879bd7a6f4178032f</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/47b1c5d1b0944aa88299f55a846fabaefc756982">git.kernel.org/stable/c/47b1c5d1b0944aa88299f55a846fabaefc756982</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/b38d2b4603fd3dda24eb8b3dd81c18a0930be97b">git.kernel.org/stable/c/b38d2b4603fd3dda24eb8b3dd81c18a0930be97b</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/a907bea273b60d3e604ec4e8e1f6c49954805794">git.kernel.org/stable/c/a907bea273b60d3e604ec4e8e1f6c49954805794</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/f1ba83755d81c6fc66ac7acd723d238f974091e9">git.kernel.org/stable/c/f1ba83755d81c6fc66ac7acd723d238f974091e9</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/0b18d1b834ab5a5009be70b530f978d7989e445b">git.kernel.org/stable/c/0b18d1b834ab5a5009be70b530f978d7989e445b</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/208669df703a25a601f45822b10c413f258bf275">git.kernel.org/stable/c/208669df703a25a601f45822b10c413f258bf275</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](#) 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](https://cve.report/api)

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