



# netfilter: nf\_tables: reject immediate NF\_QUEUE verdict

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

## Summary

<b>CVE</b>	CVE-2026-43024
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-01 15:16:46 UTC
<b>Updated</b>	2026-05-01 15:24:14 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: netfilter: nf\_tables: reject immediate NF\_QUEUE verdict n

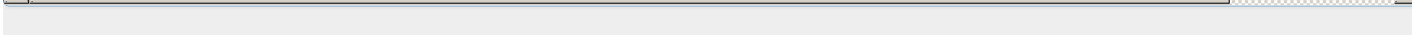
## Risk And Classification

**EPSS:** 0.000240000 probability, percentile 0.068220000 (date 2026-05-02)

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 55a60251fa50d4e68175e36666b536a602ce4f6c 2f7f825a548be55420f0f5f716f6c27b9d312d3f git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 960cf4f812530f01f6acc6878ceaa5404c06af7b f140593901724cfbd16597c3a4fcb24a58ae44b0 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 8e34430e33b8a80bc014f3efe29cac76bc30a4b4 68390437a998c3f2c57212b413abef5e6d657d88 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 6653118b176a00915125521c6572ae8e507621db 4b12a3cc3f075e750cc3c5e693fd25fb400af4a2 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected f342de4e2f33e0e39165d8639387aa6c19dff660 f710691be163ae6b39e4bcab9e5be32d329f035b git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected f342de4e2f33e0e39165d8639387aa6c19dff660 42a47f4b1b7695026ab9bc1bb35d4622b0835c95 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected f342de4e2f33e0e39165d8639387aa6c19dff660 17dc5d5a935c771338430cbc156a16a51cfd31e8 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected f342de4e2f33e0e39165d8639387aa6c19dff660 da107398cbd4bbdb6bffe2ce86d5c9384f4cec git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 8365e9d92b85fda975a5ece7a3a139cb964018c8 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 4e66422f1b56149761dc76030e6345d1cca6f869 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected f05a497e7bc8851eeeb3a58da180ba469efebb05 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 6.8
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.8 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 6.6.134 6.6.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.12.81 6.12.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.18.22 6.18.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.19.12 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/17dc5d5a935c771338430cbc156a16a51cfd31e8">git.kernel.org/stable/c/17dc5d5a935c771338430cbc156a16a51cfd31e8</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/da107398cbd4bbdb6bffe2ce86d5c9384f4cec">git.kernel.org/stable/c/da107398cbd4bbdb6bffe2ce86d5c9384f4cec</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/42a47f4b1b7695026ab9bc1bb35d4622b0835c95">git.kernel.org/stable/c/42a47f4b1b7695026ab9bc1bb35d4622b0835c95</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/68390437a998c3f2c57212b413abef5e6d657d88">git.kernel.org/stable/c/68390437a998c3f2c57212b413abef5e6d657d88</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/f710691be163ae6b39e4bcab9e5be32d329f035b">git.kernel.org/stable/c/f710691be163ae6b39e4bcab9e5be32d329f035b</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/4b12a3cc3f075e750cc3c5e693fd25fb400af4a2">git.kernel.org/stable/c/4b12a3cc3f075e750cc3c5e693fd25fb400af4a2</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/f140593901724cfbd16597c3a4fcb24a58ae44b0">git.kernel.org/stable/c/f140593901724cfbd16597c3a4fcb24a58ae44b0</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/2f7f825a548be55420f0f5f716f6c27b9d312d3f">git.kernel.org/stable/c/2f7f825a548be55420f0f5f716f6c27b9d312d3f</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)