



# netfilter: nf\_tables: flush pending destroy work before exit\_net release

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

## Summary

<b>CVE</b>	CVE-2024-35899
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-05-19 09:15:10 UTC
<b>Updated</b>	2026-05-12 12:16:40 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: netfilter: nf\_tables: flush pending destroy work before exit\_

## Risk And Classification

**Primary CVSS:** v3.1 6.1 MEDIUM from ADP

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:H

**Problem Types:** CWE-362 | CWE-362 CWE-362 Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	6.1	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	6.1	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:H

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

None

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:H

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 0935d558840099b3679c67bb7468dc78fcbad940 f4e146
CNA	Linux	Linux	affected 0935d558840099b3679c67bb7468dc78fcbad940 46c44
CNA	Linux	Linux	affected 0935d558840099b3679c67bb7468dc78fcbad940 f7e3c8
CNA	Linux	Linux	affected 0935d558840099b3679c67bb7468dc78fcbad940 4e844
CNA	Linux	Linux	affected 0935d558840099b3679c67bb7468dc78fcbad940 333b5
CNA	Linux	Linux	affected 0935d558840099b3679c67bb7468dc78fcbad940 d2c9e
CNA	Linux	Linux	affected 0935d558840099b3679c67bb7468dc78fcbad940 24cea
CNA	Linux	Linux	affected 4.20
CNA	Linux	Linux	unaffected 4.20 semver
CNA	Linux	Linux	unaffected 5.4.274 5.4.* semver
CNA	Linux	Linux	unaffected 5.10.215 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.154 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.85 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.26 6.6.* semver
CNA	Linux	Linux	unaffected 6.8.5 6.8.* semver
CNA	Linux	Linux	unaffected 6.9 * original_commit_for_fix
ADP	Linux	Linux Kernel	affected 0935d5588400 f4e14695fe80 custom
ADP	Linux	Linux Kernel	affected 0935d5588400 46c4481938e2 custom
ADP	Linux	Linux Kernel	affected 0935d5588400 f7e3c88cc2a9 custom
ADP	Linux	Linux Kernel	affected 0935d5588400 4e8447a9a3d3 custom
ADP	Linux	Linux Kernel	affected 0935d5588400 333b5085522c custom
ADP	Linux	Linux Kernel	affected 0935d5588400 d2c9eb19fc3b custom
ADP	Linux	Linux Kernel	affected 0935d5588400 24cea9677025 custom
ADP	Linux	Linux Kernel	unaffected 4.20 custom
ADP	Linux	Linux Kernel	unaffected 5.4.274 5.5.* custom

ADP	Linux	Linux Kernel	unaffected 5.4.2/4 5.5 custom
ADP	Linux	Linux Kernel	unaffected 6.8.5 6.9 custom
ADP	Linux	Linux Kernel	unaffected 6.9
ADP	Linux	Linux Kernel	affected 4.20
ADP	Linux	Linux Kernel	unaffected 5.10.215 5.11 custom
ADP	Linux	Linux Kernel	unaffected 5.15.154 5.16 custom
ADP	Linux	Linux Kernel	unaffected 6.1.85 6.2 custom
ADP	Linux	Linux Kernel	unaffected 6.6.26 6.7 custom
ADP	Siemens	SIMATIC S7-1500 TM MFP - GNU/Linux Subsystem	affected * custom

## References

Reference	Source	Link
<a href="https://lists.debian.org/debian-lts-announce/2024/06/msg00017.html">lists.debian.org/debian-lts-announce/2024/06/msg00017.html</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://lists.debian.org">lists.debian.org</a>
<a href="https://git.kernel.org/stable/c/f7e3c88cc2a977c2b9a8aa52c1ce689e7b394e49">git.kernel.org/stable/c/f7e3c88cc2a977c2b9a8aa52c1ce689e7b394e49</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/46c4481938e2ca62343b16ea83ab28f4c1733d31">git.kernel.org/stable/c/46c4481938e2ca62343b16ea83ab28f4c1733d31</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/f4e14695fe805eb0f0cb36e0ad6a560b9f985e86">git.kernel.org/stable/c/f4e14695fe805eb0f0cb36e0ad6a560b9f985e86</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://cert-portal.siemens.com/productcert/html/ssa-265688.html">cert-portal.siemens.com/productcert/html/ssa-265688.html</a>	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	<a href="https://cert-portal.siemens.com">cert-portal.siemens.com</a>
<a href="https://git.kernel.org/stable/c/24cea9677025e0de419989ecb692acd4bb34cac2">git.kernel.org/stable/c/24cea9677025e0de419989ecb692acd4bb34cac2</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/d2c9eb19fc3b11caebafde4c30a76a49203d18a6">git.kernel.org/stable/c/d2c9eb19fc3b11caebafde4c30a76a49203d18a6</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/333b5085522cf1898d5a0d92616046b414f631a7">git.kernel.org/stable/c/333b5085522cf1898d5a0d92616046b414f631a7</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/4e8447a9a3d367b5065a0b7abe101da6e0037b6e">git.kernel.org/stable/c/4e8447a9a3d367b5065a0b7abe101da6e0037b6e</a>	af854a3a-2127-422b-91ae-364da2661108	<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>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.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)