



netfilter: nf_tables: honor table dormant flag from netdev release event path

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

Summary

CVE	CVE-2024-36005
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-05-20 10:15:14 UTC
Updated	2026-05-12 12:16:46 UTC

Description In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: honor table dormant flag from netdev r

Risk And Classification

Primary CVSS: v3.1 5.5 MEDIUM from nvd@nist.gov

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

Problem Types: NVD-CWE-noinfo

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/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 d54725cd11a57c30f650260cfb0a92c268bdc
CNA	Linux	Linux	affected d54725cd11a57c30f650260cfb0a92c268bdc
CNA	Linux	Linux	affected d54725cd11a57c30f650260cfb0a92c268bdc
CNA	Linux	Linux	affected d54725cd11a57c30f650260cfb0a92c268bdc
CNA	Linux	Linux	affected d54725cd11a57c30f650260cfb0a92c268bdc
CNA	Linux	Linux	affected d54725cd11a57c30f650260cfb0a92c268bdc
CNA	Linux	Linux	affected 5.5
CNA	Linux	Linux	unaffected 5.5 semver
CNA	Linux	Linux	unaffected 5.10.216 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.158 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.90 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.30 6.6.* semver
CNA	Linux	Linux	unaffected 6.8.9 6.8.* semver
CNA	Linux	Linux	unaffected 6.9 * original_commit_for_fix
ADP	Siemens	RUGGEDCOM RST2428P	affected V3.1 custom
ADP	Siemens	SCALANCE XC-300/XR-300/XC-400/XR-500WG/XR-500 Family	unaffected * custom
ADP	Siemens	SCALANCE XCM-/XRM-/XCH-/XRH-300 Family	affected V3.1 custom
ADP	Siemens	SIMATIC S7-1500 TM MFP - GNU/Linux Subsystem	affected * custom

References

Reference	Source	Link
lists.debian.org/debian-lts-announce/2024/06/msg00017.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
git.kernel.org/stable/c/8260c980aee7d8d8a3db39faf19c391d2f898816	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/e4bb6da24de336a7899033a65490ed2d892efa5b	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/5c45feb3c288cf44a529e2657b36c259d86497d2	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
cert-portal.siemens.com/productcert/html/ssa-265688.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.co
git.kernel.org/stable/c/13ba94f6cc820fdea15efeaa17d4c722874eebf9	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
cert-portal.siemens.com/productcert/html/ssa-613116.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.co
git.kernel.org/stable/c/ca34c40d1c22c555fa7f4a21a1c807fea7290a0a	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org

git.kernel.org/stable/c/8e30abc9ace4f0add4cd761dfdbfaebae5632dd2	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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://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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report