net/sched: act_api: fix possible infinite loop in tcf_idr_check_alloc()

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2024-40995
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-07-12 13:15:20 UTC
Updated	2026-05-12 12:17:02 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: net/sched: act_api: fix possible infinite loop in tcf_idr_chec

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: CWE-835

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 0190c1d452a91c38a3462abdd81752be1b90
CNA	Linux	Linux	affected 0190c1d452a91c38a3462abdd81752be1b90
CNA	Linux	Linux	affected 0190c1d452a91c38a3462abdd81752be1b90
CNA	Linux	Linux	affected 0190c1d452a91c38a3462abdd81752be1b90
CNA	Linux	Linux	affected 0190c1d452a91c38a3462abdd81752be1b90
CNA	Linux	Linux	affected 0190c1d452a91c38a3462abdd81752be1b90
CNA	Linux	Linux	affected 0190c1d452a91c38a3462abdd81752be1b90
CNA	Linux	Linux	affected 4.19
CNA	Linux	Linux	unaffected 4.19 semver
CNA	Linux	Linux	unaffected 5.4.279 5.4.* semver
CNA	Linux	Linux	unaffected 5.10.221 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.162 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.96 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.36 6.6.* semver
CNA	Linux	Linux	unaffected 6.9.7 6.9.* semver
CNA	Linux	Linux	unaffected 6.10 * original_commit_for_fix
ADP	Siemens	RUGGEDCOM RST2428P	affected V3.1 custom
ADP	Siemens	RUGGEDCOM RST2428P	unaffected * custom
ADP	Siemens	SCALANCE XC-300/XR-300/XC-400/XR-500WG/XR-500 Family	unaffected * 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	SCALANCE XCM-/XRM-/XCH-/XRH-300 Family	unaffected * custom
ADP	Siemens	SIMATIC S7-1500 TM MFP - GNU/Linux Subsystem	affected * custom

References

Reference	Source	Link
git.kernel.org/stable/c/5f926aa96b08b6c47178fe1171e7ae331c695fc2	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/7a0e497b597df7c4cf2b63fc6e9188b6cabe5335	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/0d8a2d287c8a394c0d4653f0c6c7be4c688e5a74	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org

git.kernel.org/stable/c/25987a97eec4d5f897cd04ee1b45170829c610da	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.cc
git.kernel.org/stable/c/d864319871b05fadd153e0aede4811ca7008f5d6	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/c6a7da65a296745535a964be1019ec7691b0cb90	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.cc
cert-portal.siemens.com/productcert/html/ssa-355557.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.cc
lists.debian.org/debian-lts-announce/2025/01/msg00001.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
git.kernel.org/stable/c/6fc78d67f51aeb9a542d39a8714e16bc411582d4	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 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 registred 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

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