



mlxsw: spectrum_acl_tcam: Fix incorrect list API usage

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2024-36006
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 12:16:47 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: mlxsw: spectrum_acl_tcam: Fix incorrect list API usage B...

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 6f9579d4e3021b17b0a4cde6b04a6c94c957
CNA	Linux	Linux	affected 6f9579d4e3021b17b0a4cde6b04a6c94c957
CNA	Linux	Linux	affected 6f9579d4e3021b17b0a4cde6b04a6c94c957
CNA	Linux	Linux	affected 6f9579d4e3021b17b0a4cde6b04a6c94c957
CNA	Linux	Linux	affected 6f9579d4e3021b17b0a4cde6b04a6c94c957
CNA	Linux	Linux	affected 6f9579d4e3021b17b0a4cde6b04a6c94c957
CNA	Linux	Linux	affected 6f9579d4e3021b17b0a4cde6b04a6c94c957
CNA	Linux	Linux	affected 5.1
CNA	Linux	Linux	unaffected 5.1 semver
CNA	Linux	Linux	unaffected 5.4.275 5.4.* 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
git.kernel.org/stable/c/0b2c13b670b168e324e1cf109e67056a20fd610a	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
lists.debian.org/debian-lts-announce/2024/06/msg00017.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
git.kernel.org/stable/c/4526a56e02da3725db979358964df9cd9c567154	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/b377add0f0117409c418ddd6504bd682ebe0bf79	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/09846c2309b150b8ce4e0ce96f058197598fc530	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/ab4ecfb627338e440ae11def004c524a00d93e40	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/af8b593c3dd9df82cb199be65863af004b09fd97	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/64435b64e43d8ee60faa46c0cd04e323e8b2a7b0	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://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/cve).

Free CVE JSON API cve.report/api

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