



mlxsw: spectrum_acl_tcam: Fix warning during rehash

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

Summary

CVE	CVE-2024-36007
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 warning during rehash As

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 | CWE-noinfo Not enough information

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
3.1	ADP	DECLARED	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

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/039992b6d2df097c65f480dcf269de3d2656f573	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/743edc8547a92b6192aa1f1b6bb78233fa21dc9b	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/751d352858108314efd33ddd5a9a2b6bf7d6916	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.com
cert-portal.siemens.com/productcert/html/ssa-613116.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.com
git.kernel.org/stable/c/e890456051fe8c57944b911defb3e6de91315861	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/0b88631855026b55cad901ac28d081e0f358e596	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/1d76bd2a0034d0d08045c1c6adf2235d88982952	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/17e9e0bbae652b9b2049e51699e93dfa60b2988d	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](https://www.mitre.org/cve).

Free CVE JSON API cve.report/api

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