wifi: cfg80211: fix use-after-free in cmp_bss()

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

Summary

CVE	CVE-2025-39864
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-09-19 16:15:45 UTC
Updated	2026-05-12 13:17:16 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: wifi: cfg80211: fix use-after-free in cmp_bss() Following bs

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from nvd@nist.gov

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

Problem Types: CWE-416

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/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 3ab8227d3e7d1d2bf1829675d3197e3cb600
CNA	Linux	Linux	affected 3ab8227d3e7d1d2bf1829675d3197e3cb600
CNA	Linux	Linux	affected 3ab8227d3e7d1d2bf1829675d3197e3cb600
CNA	Linux	Linux	affected 3ab8227d3e7d1d2bf1829675d3197e3cb600
CNA	Linux	Linux	affected 3ab8227d3e7d1d2bf1829675d3197e3cb600
CNA	Linux	Linux	affected 3ab8227d3e7d1d2bf1829675d3197e3cb600
CNA	Linux	Linux	affected 3ab8227d3e7d1d2bf1829675d3197e3cb600
CNA	Linux	Linux	affected 3ab8227d3e7d1d2bf1829675d3197e3cb600
CNA	Linux	Linux	affected 5.4
CNA	Linux	Linux	unaffected 5.4 semver
CNA	Linux	Linux	unaffected 5.4.299 5.4.* semver
CNA	Linux	Linux	unaffected 5.10.243 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.192 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.151 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.105 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.46 6.12.* semver
CNA	Linux	Linux	unaffected 6.16.6 6.16.* semver
CNA	Linux	Linux	unaffected 6.17 * original_commit_for_fix
ADP	Siemens	RUGGEDCOM RST2428P	affected V3.3 custom
ADP	Siemens	SCALANCE XC-300/XR-300/XC-400/XR-500WG/XR-500 Family	affected V3.3 custom
ADP	Siemens	SCALANCE XCH328	affected V3.3 custom
ADP	Siemens	SCALANCE XCM324	affected V3.3 custom
ADP	Siemens	SCALANCE XCM328	affected V3.3 custom
ADP	Siemens	SCALANCE XCM332	affected V3.3 custom
ADP	Siemens	SCALANCE XRH334 24 V DC 8xFO CC	affected V3.3 custom
ADP	Siemens	SCALANCE XRM334 230 V AC 12xFO	affected V3.3 custom
ADP	Siemens	SCALANCE XRM334 230 V AC 8xFO	affected V3.3 custom
ADP	Siemens	SCALANCE XRM334 230V AC 2x10G 24xSFP 8xSFP	affected V3.3 custom
ADP	Siemens	SCALANCE XRM334 24 V DC 12xFO	affected V3.3 custom
ADP	Siemens	SCALANCE XRM334 24 V DC 8xFO	affected V3.3 custom

ADP	Siemens	SCALANCE XRM334 24V DC 2x10G 24xSFP 8xSFP	affected V3.3 custom
ADP	Siemens	SCALANCE XRM334 2x230 V AC 12xFO	affected V3.3 custom
ADP	Siemens	SCALANCE XRM334 2x230 V AC 8xFO	affected V3.3 custom
ADP	Siemens	SCALANCE XRM334 2x230V AC 2x10G 24xSFP 8xSFP	affected V3.3 custom
ADP	Siemens	SIMATIC CN 4100	affected V5.0 custom

References

Reference	Source	Link
lists.debian.org/debian-lts-announce/2025/10/msg00008.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
git.kernel.org/stable/c/5b7ae04969f822283a95c866967e42b4d75e0eef	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
cert-portal.siemens.com/productcert/html/ssa-089022.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.cc
git.kernel.org/stable/c/912c4b66bef713a20775cfbf3b5e9bd71525c716	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
cert-portal.siemens.com/productcert/html/ssa-032379.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.cc
git.kernel.org/stable/c/b7d08929178c16398278613df07ad65cf63cce9d	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/ff040562c10a540b8d851f7f4145fa112977f853	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/a97a9791e455bb0cd5e7a38b5abcb05523d4e21c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/6854476d9e1aeaaf05ebc98d610061c2075db07d	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/26e84445f02ce6b2fe5f3e0e28ff7add77f35e08	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
lists.debian.org/debian-lts-announce/2025/10/msg00007.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
git.kernel.org/stable/c/a8bb681e879ca3c9f722aa08d3d7ae41c42a8807	416baaa9-dc9f-4396-8d5f-8c081fb06d67	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.