wifi: mac80211: use two-phase skb reclamation in ieee80211_do_stop()

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

Summary

CVE	CVE-2024-47713
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-10-21 12:15:07 UTC
Updated	2026-05-12 12:17:15 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: use two-phase skb reclamation in ieee802

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 5061b0c2b9066de426fbc63f1278d2210e789
CNA	Linux	Linux	affected 5061b0c2b9066de426fbc63f1278d2210e789
CNA	Linux	Linux	affected 5061b0c2b9066de426fbc63f1278d2210e789
CNA	Linux	Linux	affected 5061b0c2b9066de426fbc63f1278d2210e789
CNA	Linux	Linux	affected 5061b0c2b9066de426fbc63f1278d2210e789
CNA	Linux	Linux	affected 5061b0c2b9066de426fbc63f1278d2210e789
CNA	Linux	Linux	affected 5061b0c2b9066de426fbc63f1278d2210e789
CNA	Linux	Linux	affected 5061b0c2b9066de426fbc63f1278d2210e789
CNA	Linux	Linux	affected 5061b0c2b9066de426fbc63f1278d2210e789
CNA	Linux	Linux	affected 2.6.32
CNA	Linux	Linux	unaffected 2.6.32 semver
CNA	Linux	Linux	unaffected 4.19.323 4.19.* semver
CNA	Linux	Linux	unaffected 5.4.285 5.4.* semver
CNA	Linux	Linux	unaffected 5.10.227 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.168 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.113 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.54 6.6.* semver
CNA	Linux	Linux	unaffected 6.10.13 6.10.* semver
CNA	Linux	Linux	unaffected 6.11.2 6.11.* semver
CNA	Linux	Linux	unaffected 6.12 * original_commit_for_fix
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 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/ad4b7068b101fbbb4a9ca4b99b25eb051a9482ec	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
lists.debian.org/debian-lts-announce/2025/03/msg00002.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org

git.kernel.org/stable/c/acb53a716e492a02479345157c43f21edc8bc64b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	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/9d301de12da6e1bb069a9835c38359b8e8135121	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/db5ca4b42ccfa42d2af7b335ff12578e57775c02	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/eab272972cffff9cd973b8e4055a8e81c64f7e6a	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/f232916fab67ca1c3425926df4a866e59ff26908	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/04f75f5bae33349283d6886901d9acd2f110c024	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
cert-portal.siemens.com/productcert/html/ssa-355557.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.co
git.kernel.org/stable/c/07eb0bd7b0a8abed9d45e0f567c9af1dc83e5268	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
lists.debian.org/debian-lts-announce/2025/01/msg00001.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
git.kernel.org/stable/c/058c9026ad79dc98572442fd4c7e9a36aba6f596	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.