



wifi: cfg80211: cancel wiphy_work before freeing wiphy

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

Summary

CVE	CVE-2025-21979
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-04-01 16:15:29 UTC
Updated	2026-04-06 13:39:11 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: wifi: cfg80211: cancel wiphy_work before freeing wiphy A

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 | CWE-416 CWE-416 Use After Free

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	ADP	DECLARED	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

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 ddb1bfbf4ab5c753954d0cd728253b642934a9f2 8930a3e1568cf534f86c8ed2def817c6d0528fc1 git
CNA	Linux	Linux	affected 3fcc6d7d5f40dad56dee7bde787b7e23edd4b93c 0272d4af7f92997541d8bbf4c51918b93ded6ee2 git
CNA	Linux	Linux	affected a3ee4dc84c4e9d14cb34dad095fd678127aca5b6 75d262ad3c36d52852d764588fcd887f0fcd9138 git
CNA	Linux	Linux	affected a3ee4dc84c4e9d14cb34dad095fd678127aca5b6 a5158d67bff06cb6fea31be39aeb319fd908ed8e git
CNA	Linux	Linux	affected a3ee4dc84c4e9d14cb34dad095fd678127aca5b6 dea22de162058216a90f2706f0d0b36f0ff309fd git
CNA	Linux	Linux	affected a3ee4dc84c4e9d14cb34dad095fd678127aca5b6 72d520476a2fab6f3489e8388ab524985d6c4b90 git
CNA	Linux	Linux	affected 6.5
CNA	Linux	Linux	unaffected 6.5 semver
CNA	Linux	Linux	unaffected 6.1.132 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.84 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.20 6.12.* semver
CNA	Linux	Linux	unaffected 6.13.8 6.13.* semver
CNA	Linux	Linux	unaffected 6.14 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/75d262ad3c36d52852d764588fcd887f0fcd9138	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/a5158d67bff06cb6fea31be39aeb319fd908ed8e	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/dea22de162058216a90f2706f0d0b36f0ff309fd	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/8930a3e1568cf534f86c8ed2def817c6d0528fc1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/0272d4af7f92997541d8bbf4c51918b93ded6ee2	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
lists.debian.org/debian-lts-announce/2025/05/msg00045.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org	Patch
git.kernel.org/stable/c/72d520476a2fab6f3489e8388ab524985d6c4b90	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
CVE Program record	CVE.ORG	www.cve.org	cano
NVD vulnerability detail	NVD	nvd.nist.gov	cano

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 registered 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](#)