



wifi: wilc1000: fix RCU usage in connect path

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

Summary

CVE	CVE-2024-27053
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-05-01 13:15:50 UTC
Updated	2026-05-12 12:16:31 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: wifi: wilc1000: fix RCU usage in connect path With lockdep

Risk And Classification

Primary CVSS: v3.1 9.1 CRITICAL from ADP

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

Problem Types: CWE-476 | CWE-476 CWE-476 NULL Pointer Dereference

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/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 c460495ee072fc01a9b1e8d72c179510418cafaca e55600
CNA	Linux	Linux	affected c460495ee072fc01a9b1e8d72c179510418cafaca b4bbf3
CNA	Linux	Linux	affected c460495ee072fc01a9b1e8d72c179510418cafaca d80fc4
CNA	Linux	Linux	affected c460495ee072fc01a9b1e8d72c179510418cafaca 745003
CNA	Linux	Linux	affected c460495ee072fc01a9b1e8d72c179510418cafaca 4bfd20
CNA	Linux	Linux	affected c460495ee072fc01a9b1e8d72c179510418cafaca 5800ec
CNA	Linux	Linux	affected c460495ee072fc01a9b1e8d72c179510418cafaca dd50d3
CNA	Linux	Linux	affected c460495ee072fc01a9b1e8d72c179510418cafaca 205c50
CNA	Linux	Linux	affected 5.1
CNA	Linux	Linux	unaffected 5.1 semver
CNA	Linux	Linux	unaffected 5.4.273 5.4.* semver
CNA	Linux	Linux	unaffected 5.10.214 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.153 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.83 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.23 6.6.* semver
CNA	Linux	Linux	unaffected 6.7.11 6.7.* semver
CNA	Linux	Linux	unaffected 6.8.2 6.8.* semver
CNA	Linux	Linux	unaffected 6.9 * original_commit_for_fix
ADP	Linux	Linux Kernel	affected c460495ee072 e556006de4ea custom
ADP	Linux	Linux Kernel	affected c460495ee072 b4bbf38c350a custom
ADP	Linux	Linux Kernel	affected c460495ee072 d80fc436751c custom
ADP	Linux	Linux Kernel	affected c460495ee072 745003b5917b custom
ADP	Linux	Linux Kernel	affected c460495ee072 4bfd20d5f5c custom
ADP	Linux	Linux Kernel	affected c460495ee072 5800ec78775c custom
ADP	Linux	Linux Kernel	affected c460495ee072 dd50d3ead6e3 custom
ADP	Linux	Linux Kernel	affected c460495ee072 205c50306acf custom

ADP	Linux	Linux Kernel	unaffected 5.4.273 5.5 custom
ADP	Linux	Linux Kernel	unaffected 5.15.153 5.16 custom
ADP	Linux	Linux Kernel	unaffected 6.1.83 6.2 custom
ADP	Linux	Linux Kernel	unaffected 6.6.23 6.7 custom
ADP	Linux	Linux Kernel	unaffected 6.7.11 6.8 custom
ADP	Linux	Linux Kernel	unaffected 6.9
ADP	Linux	Linux Kernel	unaffected 5.1 custom
ADP	Linux	Linux Kernel	affected 5.1
ADP	Linux	Linux Kernel	unaffected 5.10.214 5.11 custom
ADP	Linux	Linux Kernel	unaffected 6.8.2 6.9 custom
ADP	Siemens	SIMATIC S7-1500 TM MFP - GNU/Linux Subsystem	affected * custom

References

Reference	Source	Link
lists.debian.org/debian-lts-announce/2024/06/msg00017.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
git.kernel.org/stable/c/205c50306acf58a335eb19fa84e40140f4fe814f	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/4bfd20d5f5c62b5495d6c0016ee6933bd3add7ce	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
git.kernel.org/stable/c/d80fc436751cfa6b02a8eda74eb6cce7dadfe5a2	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/e556006de4ea93abe2b46cba202a2556c544b8b2	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/b4bbf38c350acb6500cbe667b1e2e68f896e4b38	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/745003b5917b610352f52fe0d11ef658d6471ec2	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/5800ec78775c0cd646f71eb9bf8402fb794807de	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/dd50d3ead6e3707bb0a5df7cc832730c93ace3a7	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 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