



wifi: rtw88: always wait for both firmware loading attempts

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

Summary

CVE	CVE-2024-47718
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-10-21 12:15:08 UTC
Updated	2026-05-12 12:17:15 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: wifi: rtw88: always wait for both firmware loading attempts

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 c8e5695eae9959fc5774c0f490f2450be8bad
CNA	Linux	Linux	affected c8e5695eae9959fc5774c0f490f2450be8bad
CNA	Linux	Linux	affected c8e5695eae9959fc5774c0f490f2450be8bad
CNA	Linux	Linux	affected c8e5695eae9959fc5774c0f490f2450be8bad
CNA	Linux	Linux	affected c8e5695eae9959fc5774c0f490f2450be8bad
CNA	Linux	Linux	affected c8e5695eae9959fc5774c0f490f2450be8bad
CNA	Linux	Linux	affected c8e5695eae9959fc5774c0f490f2450be8bad
CNA	Linux	Linux	affected 5.6
CNA	Linux	Linux	unaffected 5.6 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/ceaab3fb64d6a5426a3db8f87f3e5757964f2532	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/a0c1e2da652cf70825739bc12d49ea15805690bf	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/e9a78d9417e167410d6fb83c4e908b077ad8ba6d	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/0e735a4c6137262bcefe45bb52fde7b1f5fc6c4d	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
lists.debian.org/debian-lts-announce/2025/01/msg00001.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
git.kernel.org/stable/c/1b8178a2ae272256ea0dc4f940320a81003535e2	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/9432185540bafd42b7bfac6e6ef2f0a0fb4be447	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/7887ad11995a4142671cc49146db536f923c8568	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.

© [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