



wifi: wlcore: Return -ENOMEM instead of -EAGAIN if there is not enough headroom

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

Summary

CVE	CVE-2026-31552
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-24 15:16:29 UTC
Updated	2026-04-27 20:15:16 UTC

Description In the Linux kernel, the following vulnerability has been resolved: wifi: wlcore: Return -ENOMEM instead of -EAGAIN if there

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

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

EPSS: 0.000240000 probability, percentile 0.067850000 (date 2026-04-27)

Problem Types: CWE-835

Version	Source	Type	Score	Severity	Vector
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	CNA	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/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 88295a55fefe5414e64293638b6f7549646e58ed 980f793645540ca7a6318165cc12f49d5febeb99 git
CNA	Linux	Linux	affected cd89a4656c03f8db0c57350aaec69cd3cfaa3522 12f9eef39e49716c763714bfda835a733d5f6dea git
CNA	Linux	Linux	affected 745a0810dbc96a0471e5f5e627ba1e978c3116d4 ceb46b40b021d21911ff8608ce4ed33c1264ad2f git
CNA	Linux	Linux	affected b167312390fdd461c81ead516f2b0b44e83a9edb a6dc74209462c4fe5a88718d2f3a5286886081c8 git
CNA	Linux	Linux	affected 71de0b6e04bbee5575caf9a1e4d424e7dcc50018 cfa64e2b3717be1da7c4c1aff7268a009e8c1610 git
CNA	Linux	Linux	affected 689a7980e4788e13e766763d53569fb78dea2513 46c670ff1ff466e5eccb3940f726586473dc053c git
CNA	Linux	Linux	affected e75665dd096819b1184087ba5718bd93beaff51 f2c06d718a7b85cbc59ceaa2ff3f46b178ac709c git
CNA	Linux	Linux	affected e75665dd096819b1184087ba5718bd93beaff51 deb353d9bb009638b7762cae2d0b6e8fdbb41a69 git
CNA	Linux	Linux	affected 6.19
CNA	Linux	Linux	unaffected 6.19 semver
CNA	Linux	Linux	unaffected 5.10.253 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.203 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.167 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.130 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.78 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.20 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.10 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/a6dc74209462c4fe5a88718d2f3a5286886081c8	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/deb353d9bb009638b7762cae2d0b6e8fdbb41a69	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/ceb46b40b021d21911ff8608ce4ed33c1264ad2f	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch

git.kernel.org/stable/c/12f9eef39e49716c763714bfda835a733d5f6dea	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/f2c06d718a7b85cbc59ceaa2ff3f46b178ac709c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/46c670ff1ff466e5eccb3940f726586473dc053c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/980f793645540ca7a6318165cc12f49d5febeb99	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/cfa64e2b3717be1da7c4c1aff7268a009e8c1610	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

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