



wifi: mac80211: Fix static_branch_dec() underflow for aql_disable.

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2026-31551 |
| 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 20:15:30 UTC |

Description In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: Fix static_branch_dec() underflow for aql_

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

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

Problem Types: CWE-191

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 e908435e402aff23c9b0b3c59c7cd12b08b681b0 787152497ac763deab16f6f4b7ce79aaeb3eb7e8 git |
| CNA | Linux | Linux | affected e908435e402aff23c9b0b3c59c7cd12b08b681b0 8bb90ff77326c34e75b573b1febdd9586fec5aba git |
| CNA | Linux | Linux | affected e908435e402aff23c9b0b3c59c7cd12b08b681b0 256f7d4c11235d0569f78413c41dc89d2dc1557c git |
| CNA | Linux | Linux | affected e908435e402aff23c9b0b3c59c7cd12b08b681b0 29a1a350afcd28a2150bd73b8bd83eac3480f13e git |
| CNA | Linux | Linux | affected e908435e402aff23c9b0b3c59c7cd12b08b681b0 5ba05436f15d16ae7ab04b880e8bf8d440be892b git |
| CNA | Linux | Linux | affected e908435e402aff23c9b0b3c59c7cd12b08b681b0 b24763d32d5b4ada766deca4b42d6766272fef0c git |
| CNA | Linux | Linux | affected e908435e402aff23c9b0b3c59c7cd12b08b681b0 b94ae8e0d5fe1bdbbfdc3854ff6ce98f6876a828 git |
| CNA | Linux | Linux | affected 5.12 |
| CNA | Linux | Linux | unaffected 5.12 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/8bb90ff77326c34e75b573b1febdd9586fec5aba | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | Patch |
| git.kernel.org/stable/c/5ba05436f15d16ae7ab04b880e8bf8d440be892b | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | Patch |
| git.kernel.org/stable/c/256f7d4c11235d0569f78413c41dc89d2dc1557c | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | Patch |
| git.kernel.org/stable/c/b94ae8e0d5fe1bdbbfdc3854ff6ce98f6876a828 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | Patch |
| git.kernel.org/stable/c/29a1a350afcd28a2150bd73b8bd83eac3480f13e | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | Patch |
| git.kernel.org/stable/c/787152497ac763deab16f6f4b7ce79aaeb3eb7e8 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | Patch |
| git.kernel.org/stable/c/b24763d32d5b4ada766deca4b42d6766272fef0c | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | Patch |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical |

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](#)