



# staging: rtl8723bs: fix potential out-of-bounds read in rtw\_restruct\_wmm\_ie

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

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2026-43386                               |
| <b>State</b>           | PUBLISHED                                    |
| <b>Assigner</b>        | Linux  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback |
| <b>Published</b>       | 2026-05-08 15:16:49 UTC                      |
| <b>Updated</b>         | 2026-05-12 14:10:27 UTC                      |

**Description** In the Linux kernel, the following vulnerability has been resolved: staging: rtl8723bs: fix potential out-of-bounds read in rtw\_

## Risk And Classification

**EPSS:** 0.000240000 probability, percentile 0.070360000 (date 2026-05-12)

## Vendor Declared Affected Products

| Source | Vendor | Product | Version  |
|--------|--------|---------|--|
| CNA    | Linux  | Linux   | affected 554c0a3abf216c991c5ebddcdb2c08689ecd290b 6ff2243d5e05a5239e39d4ba61d96b0ea3bf7259 git |
| CNA    | Linux  | Linux   | affected 554c0a3abf216c991c5ebddcdb2c08689ecd290b 12cc6e8f8d4245b7b5a408c6fc8ab1d098d67020 git |
| CNA    | Linux  | Linux   | affected 554c0a3abf216c991c5ebddcdb2c08689ecd290b 209644e25757c499e1c1f08c071ea0386d4448b6 gi  |
| CNA    | Linux  | Linux   | affected 554c0a3abf216c991c5ebddcdb2c08689ecd290b 768f25613a9fe6766d15a4a72979657adfc1c6d8 git |
| CNA    | Linux  | Linux   | affected 554c0a3abf216c991c5ebddcdb2c08689ecd290b e14a1148f02e8cf1ca380d57e4b95ca36c97f45d git |
| CNA    | Linux  | Linux   | affected 554c0a3abf216c991c5ebddcdb2c08689ecd290b 4dd2d9cf563c54e09d5f7eacf95c5b8f538b513b git |
| CNA    | Linux  | Linux   | affected 554c0a3abf216c991c5ebddcdb2c08689ecd290b d97fc1b29513010b60fde874c7f0ba816744e18c git |
| CNA    | Linux  | Linux   | affected 554c0a3abf216c991c5ebddcdb2c08689ecd290b a75281626fc8fa6dc6c9cc314ee423e8bc45203b git |
| CNA    | Linux  | Linux   | affected 4.12  |
| CNA    | Linux  | Linux   | unaffected 4.12 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 6.18.19 6.18.* semver   |

|     |                       |                       |  |
|-----|-----------------------|-----------------------|--|
| CNA | <a href="#">Linux</a> | <a href="#">Linux</a> | unaffected 6.19.9 6.19.* semver          |
| CNA | <a href="#">Linux</a> | <a href="#">Linux</a> | unaffected 7.0 * original_commit_for_fix |

## References

| Reference   | Source                               | Link  | Tags      |
|---|--------------------------------------|---|-----------|
| <a href="https://git.kernel.org/stable/c/d97fc1b29513010b60fde874c7f0ba816744e18c">git.kernel.org/stable/c/d97fc1b29513010b60fde874c7f0ba816744e18c</a> | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org">git.kernel.org</a> |           |
| <a href="https://git.kernel.org/stable/c/e14a1148f02e8cf1ca380d57e4b95ca36c97f45d">git.kernel.org/stable/c/e14a1148f02e8cf1ca380d57e4b95ca36c97f45d</a> | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org">git.kernel.org</a> |           |
| <a href="https://git.kernel.org/stable/c/4dd2d9cf563c54e09d5f7eacf95c5b8f538b513b">git.kernel.org/stable/c/4dd2d9cf563c54e09d5f7eacf95c5b8f538b513b</a> | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org">git.kernel.org</a> |           |
| <a href="https://git.kernel.org/stable/c/6ff2243d5e05a5239e39d4ba61d96b0ea3bf7259">git.kernel.org/stable/c/6ff2243d5e05a5239e39d4ba61d96b0ea3bf7259</a> | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org">git.kernel.org</a> |           |
| <a href="https://git.kernel.org/stable/c/a75281626fc8fa6dc6c9cc314ee423e8bc45203b">git.kernel.org/stable/c/a75281626fc8fa6dc6c9cc314ee423e8bc45203b</a> | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org">git.kernel.org</a> |           |
| <a href="https://git.kernel.org/stable/c/768f25613a9fe6766d15a4a72979657adfc1c6d8">git.kernel.org/stable/c/768f25613a9fe6766d15a4a72979657adfc1c6d8</a> | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org">git.kernel.org</a> |           |
| <a href="https://git.kernel.org/stable/c/12cc6e8f8d4245b7b5a408c6fc8ab1d098d67020">git.kernel.org/stable/c/12cc6e8f8d4245b7b5a408c6fc8ab1d098d67020</a> | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org">git.kernel.org</a> |           |
| <a href="https://git.kernel.org/stable/c/209644e25757c499e1c1f08c071ea0386d4448b6">git.kernel.org/stable/c/209644e25757c499e1c1f08c071ea0386d4448b6</a> | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org">git.kernel.org</a> |           |
| CVE Program record  | CVE.ORG                              | <a href="https://www.cve.org">www.cve.org</a>       | canonical |
| NVD vulnerability detail  | NVD                                  | <a href="https://nvd.nist.gov">nvd.nist.gov</a>     | 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](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)