



# staging: rtl8723bs: properly validate the data in rtw\_get\_ie\_ex()

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

## Summary

<b>CVE</b>	CVE-2026-43387
<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 15:16:50 UTC
<b>Updated</b>	2026-05-12 14:10:27 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: staging: rtl8723bs: properly validate the data in rtw\_get\_ie

## Risk And Classification

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

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 554c0a3abf216c991c5ebddcdb2c08689ecd290b ac38856092b4c994f94343251b30520bdeb7f475 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 554c0a3abf216c991c5ebddcdb2c08689ecd290b 35969c3a208a07cb8642301df5869c34e2db7071 gi
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 554c0a3abf216c991c5ebddcdb2c08689ecd290b 8097a48c606a9306281ea7bd73bf2afc97553733 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 554c0a3abf216c991c5ebddcdb2c08689ecd290b 740bca8bbdb707c0e4bb11e3316deb2f04fc7ce1 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 554c0a3abf216c991c5ebddcdb2c08689ecd290b 821f7d759fb2de33c5e5b0c4981181c4d0c3e9b1 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 554c0a3abf216c991c5ebddcdb2c08689ecd290b 6d62fa548387e159a21ea95132c09bfc96d336ed git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 554c0a3abf216c991c5ebddcdb2c08689ecd290b 9a4cd4c37593cc8b8d28f9a6732b490a8032006a gi
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 554c0a3abf216c991c5ebddcdb2c08689ecd290b f0109b9d3e1e455429279d602f6276e34689750a gi
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 4.12
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 4.12 semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 5.10.253 5.10.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 5.15.203 5.15.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.1.167 6.1.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.6.130 6.6.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.12.78 6.12.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	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/6d62fa548387e159a21ea95132c09bfc96d336ed">git.kernel.org/stable/c/6d62fa548387e159a21ea95132c09bfc96d336ed</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/f0109b9d3e1e455429279d602f6276e34689750a">git.kernel.org/stable/c/f0109b9d3e1e455429279d602f6276e34689750a</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/35969c3a208a07cb8642301df5869c34e2db7071">git.kernel.org/stable/c/35969c3a208a07cb8642301df5869c34e2db7071</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/ac38856092b4c994f94343251b30520bdeb7f475">git.kernel.org/stable/c/ac38856092b4c994f94343251b30520bdeb7f475</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/8097a48c606a9306281ea7bd73bf2afc97553733">git.kernel.org/stable/c/8097a48c606a9306281ea7bd73bf2afc97553733</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/740bca8bbdb707c0e4bb11e3316deb2f04fc7ce1">git.kernel.org/stable/c/740bca8bbdb707c0e4bb11e3316deb2f04fc7ce1</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/9a4cd4c37593cc8b8d28f9a6732b490a8032006a">git.kernel.org/stable/c/9a4cd4c37593cc8b8d28f9a6732b490a8032006a</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/821f7d759fb2de33c5e5b0c4981181c4d0c3e9b1">git.kernel.org/stable/c/821f7d759fb2de33c5e5b0c4981181c4d0c3e9b1</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)