staging: rtl8723bs: fix memory leak on failure path

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-43225
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-06 12:16:42 UTC
Updated	2026-05-08 21:22:38 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: staging: rtl8723bs: fix memory leak on failure path cfg802

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

Problem Types: CWE-401

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 554c0a3abf216c991c5ebddcdb2c08689ecd290b 9874e33ce52ba449ab0ade78752a2d37a2294617 g
CNA	Linux	Linux	affected 554c0a3abf216c991c5ebddcdb2c08689ecd290b a968c6a39607c129b8ac2c3c2a5e8923574e90d0 gi
CNA	Linux	Linux	affected 554c0a3abf216c991c5ebddcdb2c08689ecd290b 8311bb40698ba027649d5d1ca84ad4bf25270546 gi
CNA	Linux	Linux	affected 554c0a3abf216c991c5ebddcdb2c08689ecd290b 9f70f78e22b321429afc77befecedf05543d4e2c git
CNA	Linux	Linux	affected 554c0a3abf216c991c5ebddcdb2c08689ecd290b af48c1a0abe849e167fc754b6c260b6d8350b6fd git
CNA	Linux	Linux	affected 554c0a3abf216c991c5ebddcdb2c08689ecd290b 017295b17bf1f477246c95bd253a7ef0cb4684c9 git
CNA	Linux	Linux	affected 554c0a3abf216c991c5ebddcdb2c08689ecd290b abe850d82c8cb72d28700673678724e779b1826e g
CNA	Linux	Linux	affected 4.12
CNA	Linux	Linux	unaffected 4.12 semver
CNA	Linux	Linux	unaffected 5.15.202 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.165 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.128 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.75 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.16 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.6 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/017295b17bf1f477246c95bd253a7ef0cb4684c9	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/8311bb40698ba027649d5d1ca84ad4bf25270546	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/af48c1a0abe849e167fc754b6c260b6d8350b6fd	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/a968c6a39607c129b8ac2c3c2a5e8923574e90d0	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/9f70f78e22b321429afc77befecedf05543d4e2c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/9874e33ce52ba449ab0ade78752a2d37a2294617	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/abe850d82c8cb72d28700673678724e779b1826e	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 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 registred 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**