



# wifi: brcmfmac: Fix potential kernel oops when probe fails

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

## Summary

<b>CVE</b>	CVE-2026-43144
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-06 12:16:31 UTC
<b>Updated</b>	2026-05-06 13:07:51 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: wifi: brcmfmac: Fix potential kernel oops when probe fails

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 0ff0843310b74e565901d85f849fb308c3b1f220 64ccb0aac41c5055780c2a58bbe2c1b362ceccde git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 0ff0843310b74e565901d85f849fb308c3b1f220 379aac7ee8240848aa35f605b06addb4617c863e git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 0ff0843310b74e565901d85f849fb308c3b1f220 243307a0d1b0d01538e202c00454c28b21d4432e git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 6.13
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.13 semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.18.16 6.18.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.19.6 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/379aac7ee8240848aa35f605b06addb4617c863e">git.kernel.org/stable/c/379aac7ee8240848aa35f605b06addb4617c863e</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/243307a0d1b0d01538e202c00454c28b21d4432e">git.kernel.org/stable/c/243307a0d1b0d01538e202c00454c28b21d4432e</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/64ccb0aac41c5055780c2a58bbe2c1b362ceccde">git.kernel.org/stable/c/64ccb0aac41c5055780c2a58bbe2c1b362ceccde</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>	canonic
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	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 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](#)