



# pmdomain: bcm: bcm2835-power: Increase ASB control timeout

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

## Summary

<b>CVE</b>	CVE-2026-31550
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-24 15:16:29 UTC
<b>Updated</b>	2026-04-24 17:51:40 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: pmdomain: bcm: bcm2835-power: Increase ASB control ti

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 670c672608a1ffc7ac0f872734843593bb8b15 0e84e74849d2d7e9b23a09c2d5e0d9357db1ca59 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 670c672608a1ffc7ac0f872734843593bb8b15 c5e734f6a0740dce92e7c919e632cb43fa5d4e53 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 670c672608a1ffc7ac0f872734843593bb8b15 622ab02e955c35c125ff2b65d8327b2c52db8758 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 670c672608a1ffc7ac0f872734843593bb8b15 9443202d91388026dbf7312972a74fbfd27ee82f git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 670c672608a1ffc7ac0f872734843593bb8b15 ea4fa54b83bb2e4a21e9026824bfe271b1a6ee1e git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 670c672608a1ffc7ac0f872734843593bb8b15 18605b1b936b66b1f34dcf8e9ad4f1fbcf7a7c13 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 670c672608a1ffc7ac0f872734843593bb8b15 572f17180f26619809b8e0593d926762aa8660ff git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 670c672608a1ffc7ac0f872734843593bb8b15 b826d2c0b0ecb844c84431ba6b502e744f5d919a git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 5.1
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 5.1 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 6.18.20 6.18.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.19.10 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/b826d2c0b0ecb844c84431ba6b502e744f5d919a">git.kernel.org/stable/c/b826d2c0b0ecb844c84431ba6b502e744f5d919a</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/9443202d91388026dbf7312972a74fbfd27ee82f">git.kernel.org/stable/c/9443202d91388026dbf7312972a74fbfd27ee82f</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/c5e734f6a0740dce92e7c919e632cb43fa5d4e53">git.kernel.org/stable/c/c5e734f6a0740dce92e7c919e632cb43fa5d4e53</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/572f17180f26619809b8e0593d926762aa8660ff">git.kernel.org/stable/c/572f17180f26619809b8e0593d926762aa8660ff</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/18605b1b936b66b1f34dcf8e9ad4f1fbcf7a7c13">git.kernel.org/stable/c/18605b1b936b66b1f34dcf8e9ad4f1fbcf7a7c13</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/ea4fa54b83bb2e4a21e9026824bfe271b1a6ee1e">git.kernel.org/stable/c/ea4fa54b83bb2e4a21e9026824bfe271b1a6ee1e</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/0e84e74849d2d7e9b23a09c2d5e0d9357db1ca59">git.kernel.org/stable/c/0e84e74849d2d7e9b23a09c2d5e0d9357db1ca59</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/622ab02e955c35c125ff2b65d8327b2c52db8758">git.kernel.org/stable/c/622ab02e955c35c125ff2b65d8327b2c52db8758</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](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/cve).

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)