



# net: usb: aqc111: Do not perform PM inside suspend callback

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

## Summary

<b>CVE</b>	CVE-2026-23446
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-03 16:16:30 UTC
<b>Updated</b>	2026-04-07 13:21:09 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: net: usb: aqc111: Do not perform PM inside suspend callb

## Risk And Classification

**EPSS:** 0.000240000 probability, percentile 0.066190000 (date 2026-04-07)

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected e58ba4544c7771591d1e3157bc01b4a8e4d1c3fc 621f2f43741b51f62d767eb4752fbcfe2526926 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected e58ba4544c7771591d1e3157bc01b4a8e4d1c3fc 4de6a43e8ecf961feabddf0e9d6911081d2ed218 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected e58ba4544c7771591d1e3157bc01b4a8e4d1c3fc 3267bcb744ee8a2feabaa7ab69473f086f67fd71 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected e58ba4544c7771591d1e3157bc01b4a8e4d1c3fc d3e32a612c6391ca9b7c183aeec22b4fd24c300c gi
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected e58ba4544c7771591d1e3157bc01b4a8e4d1c3fc 98e8aed64614b0c199d5f0391fbe1a4331cb5773 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected e58ba4544c7771591d1e3157bc01b4a8e4d1c3fc 069c8f5aebe4d5224cf62acc7d4b3486091c658a git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 5.0
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 5.0 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-rc5 * original_commit_for_fix

## References

Reference	Source	Link	Tags
git.kernel.org/stable/c/3267bcb744ee8a2feabaa7ab69473f086f67fd71	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
git.kernel.org/stable/c/d3e32a612c6391ca9b7c183aeec22b4fd24c300c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
git.kernel.org/stable/c/069c8f5aeb4d5224cf62acc7d4b3486091c658a	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
git.kernel.org/stable/c/4de6a43e8ecf961feabddf0e9d6911081d2ed218	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
git.kernel.org/stable/c/98e8aed64614b0c199d5f0391fbe1a4331cb5773	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
git.kernel.org/stable/c/621f2f43741b51f62d767eb4752fbcefe2526926	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](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). This site includes MITRE data granted under the following [license](https://mitre.org).

**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)