



media: venus: protect against spurious interrupts during probe

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

Summary

CVE	CVE-2025-39709
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-09-05 18:15:48 UTC
Updated	2026-05-12 13:17:06 UTC

Description In the Linux kernel, the following vulnerability has been resolved: media: venus: protect against spurious interrupts during p

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-476

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 af2c3834c8ca7cc65d15592ac671933df8848115 18c2b2bd982b8546312c9a78955156721
CNA	Linux	Linux	affected af2c3834c8ca7cc65d15592ac671933df8848115 88cf63c2599761c48dec8f618d57dccf8f6f
CNA	Linux	Linux	affected af2c3834c8ca7cc65d15592ac671933df8848115 9db6a78bc5e418e0064e2248c8f3b9b9e8
CNA	Linux	Linux	affected af2c3834c8ca7cc65d15592ac671933df8848115 37cc0ac889b018097c217c5929fd6dc2ae
CNA	Linux	Linux	affected af2c3834c8ca7cc65d15592ac671933df8848115 f54be97bc69b1096198b6717c150dec69f
CNA	Linux	Linux	affected af2c3834c8ca7cc65d15592ac671933df8848115 639eb587f977c02423f4762467055b2390
CNA	Linux	Linux	affected af2c3834c8ca7cc65d15592ac671933df8848115 e796028b4835af00d9a38ebbb208ec3a6f
CNA	Linux	Linux	affected af2c3834c8ca7cc65d15592ac671933df8848115 3200144a2fa4209dc084a19941b9b203b4
CNA	Linux	Linux	affected 4.13
CNA	Linux	Linux	unaffected 4.13 semver
CNA	Linux	Linux	unaffected 5.4.297 5.4.* semver
CNA	Linux	Linux	unaffected 5.10.241 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.190 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.149 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.103 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.44 6.12.* semver
CNA	Linux	Linux	unaffected 6.16.4 6.16.* semver
CNA	Linux	Linux	unaffected 6.17 * original_commit_for_fix
ADP	Siemens	SIMATIC CN 4100	affected V5.0 custom

References

Reference	Source	Link
lists.debian.org/debian-lts-announce/2025/10/msg00008.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
git.kernel.org/stable/c/f54be97bc69b1096198b6717c150dec69f2a1b4d	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/18c2b2bd982b8546312c9a7895515672169f28e0	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/e796028b4835af00d9a38ebbb208ec3a6634702a	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/88cf63c2599761c48dec8f618d57dccf8f6f4b53	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
cert-portal.siemens.com/productcert/html/ssa-032379.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.co
git.kernel.org/stable/c/3200144a2fa4209dc084a19941b9b203b43580f0	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org

git.kernel.org/stable/c/9db6a78bc5e418e0064e2248c8f3b9b9e8418646	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/37cc0ac889b018097c217c5929fd6dc2aed636a1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
lists.debian.org/debian-lts-announce/2025/10/msg00007.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
git.kernel.org/stable/c/639eb587f977c02423f4762467055b23902b4131	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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/licenses).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report