media: venus: Fix OOB read due to missing payload bound check

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

Summary

CVE	CVE-2025-38679
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-09-04 16:15:35 UTC
Updated	2026-05-12 13:16:54 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: media: venus: Fix OOB read due to missing payload boun

Risk And Classification

Primary CVSS: v3.1 7.1 HIGH from nvd@nist.gov

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H

Problem Types: CWE-125

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/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 09c2845e8fe4fcab942929480203f504a6e0a114 a3eef5847603cd8a4110587907988c3f93
CNA	Linux	Linux	affected 09c2845e8fe4fcab942929480203f504a6e0a114 8f274e2b05fdae7a53cee83979202b5ecb
CNA	Linux	Linux	affected 09c2845e8fe4fcab942929480203f504a6e0a114 6f08bfb5805637419902f3d70069fe17a40
CNA	Linux	Linux	affected 09c2845e8fe4fcab942929480203f504a6e0a114 c956c3758510b448b3d4d10d1da8230e8
CNA	Linux	Linux	affected 09c2845e8fe4fcab942929480203f504a6e0a114 bed4921055dd7bb4d2eea2729852ae18c
CNA	Linux	Linux	affected 09c2845e8fe4fcab942929480203f504a6e0a114 06d6770ff0d8cc8dfd392329a8cc03e2a83
CNA	Linux	Linux	affected 4.13
CNA	Linux	Linux	unaffected 4.13 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 6.12.43 6.12.* semver
CNA	Linux	Linux	unaffected 6.15.11 6.15.* semver
CNA	Linux	Linux	unaffected 6.16.2 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
git.kernel.org/stable/c/c956c3758510b448b3d4d10d1da8230e8c9bf668	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
lists.debian.org/debian-lts-announce/2025/10/msg00008.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
git.kernel.org/stable/c/bed4921055dd7bb4d2eea2729852ae18cf97a2c6	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/8f274e2b05fdae7a53cee83979202b5ecb49035c	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/a3eef5847603cd8a4110587907988c3f93c9605a	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/06d6770ff0d8cc8dfd392329a8cc03e2a83e7289	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/6f08bfb5805637419902f3d70069fe17a404545b	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.

Free CVE JSON API cve.report/api

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