ALSA: usb-audio: Validate UAC3 cluster segment descriptors

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

Summary

CVE	CVE-2025-39757
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-09-11 17:15:39 UTC
Updated	2026-05-12 13:17:09 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: ALSA: usb-audio: Validate UAC3 cluster segment descrip

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 11785ef53228d23ec386f5fe4a34601536f0c891 799c06ad4c9c790c265e8b6b94947213f1
CNA	Linux	Linux	affected 11785ef53228d23ec386f5fe4a34601536f0c891 786571b10b1ae6d90e1242848ce78ee7e
CNA	Linux	Linux	affected 11785ef53228d23ec386f5fe4a34601536f0c891 275e37532e8ebe25e8a4069b2d9f955bfd
CNA	Linux	Linux	affected 11785ef53228d23ec386f5fe4a34601536f0c891 47ab3d820cb0a502bd0074f83bb3cf7ab5
CNA	Linux	Linux	affected 11785ef53228d23ec386f5fe4a34601536f0c891 1034719fdefd26caeec0a44a868bb5a412
CNA	Linux	Linux	affected 11785ef53228d23ec386f5fe4a34601536f0c891 ae17b3b5e753efc239421d186cd1ff06e5a
CNA	Linux	Linux	affected 11785ef53228d23ec386f5fe4a34601536f0c891 dfdcbcde5c20df878178245d4449feada7d
CNA	Linux	Linux	affected 11785ef53228d23ec386f5fe4a34601536f0c891 7ef3fd250f84494fb2f7871f357808edaa1fc
CNA	Linux	Linux	affected 11785ef53228d23ec386f5fe4a34601536f0c891 ecfd41166b72b67d3bdeb88d224ff445f616
CNA	Linux	Linux	affected 4.19
CNA	Linux	Linux	unaffected 4.19 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 6.12.43 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/799c06ad4c9c790c265e8b6b94947213f1fb389c	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/47ab3d820cb0a502bd0074f83bb3cf7ab5d79902	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/dfdcbcde5c20df878178245d4449feada7d5b201	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/ae17b3b5e753efc239421d186cd1ff06e5ac296e	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org

git.kernel.org/stable/c/786571b10b1ae6d90e1242848ce78ee7e1d493c4	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/7ef3fd250f84494fb2f7871f357808edaa1fc6ce	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/1034719fdefd26caeec0a44a868bb5a412c2c1a5	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.cc
git.kernel.org/stable/c/275e37532e8ebe25e8a4069b2d9f955bfd202a46	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/ecfd41166b72b67d3bdeb88d224ff445f6163869	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
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.