



# ALSA: usb-audio: Validate UAC3 cluster segment descriptors

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

## Summary

<b>CVE</b>	CVE-2025-39757
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-09-11 17:15:39 UTC
<b>Updated</b>	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 799c06ad4c9c790c265e8b6b94947213f11
CNA	Linux	Linux	affected 11785ef53228d23ec386f5fe4a34601536f0c891 786571b10b1ae6d90e1242848ce78ee7e1
CNA	Linux	Linux	affected 11785ef53228d23ec386f5fe4a34601536f0c891 275e37532e8e8e25e8a4069b2d9f955bfd2
CNA	Linux	Linux	affected 11785ef53228d23ec386f5fe4a34601536f0c891 47ab3d820cb0a502bd0074f83bb3cf7ab5c
CNA	Linux	Linux	affected 11785ef53228d23ec386f5fe4a34601536f0c891 1034719fdefd26caeec0a44a868bb5a412c
CNA	Linux	Linux	affected 11785ef53228d23ec386f5fe4a34601536f0c891 ae17b3b5e753efc239421d186cd1ff06e5a
CNA	Linux	Linux	affected 11785ef53228d23ec386f5fe4a34601536f0c891 dfdcbcde5c20df878178245d4449feada7d
CNA	Linux	Linux	affected 11785ef53228d23ec386f5fe4a34601536f0c891 7ef3fd250f84494fb2f7871f357808edaa1fc
CNA	Linux	Linux	affected 11785ef53228d23ec386f5fe4a34601536f0c891 ecf41166b72b67d3bdeb88d224ff445f616
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	<a href="https://git.kernel.org">git.kernel.org</a>
lists.debian.org/debian-lts-announce/2025/10/msg00008.html	af854a3a-2127-422b-91ae-364da2661108	<a href="https://lists.debian.org">lists.debian.org</a>
git.kernel.org/stable/c/47ab3d820cb0a502bd0074f83bb3cf7ab5d79902	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
git.kernel.org/stable/c/dfdcbcde5c20df878178245d4449feada7d5b201	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
git.kernel.org/stable/c/ae17b3b5e753efc239421d186cd1ff06e5ac296e	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>

<a href="https://git.kernel.org/stable/c/786571b10b1ae6d90e1242848ce78ee7e1d493c4">git.kernel.org/stable/c/786571b10b1ae6d90e1242848ce78ee7e1d493c4</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/7ef3fd250f84494fb2f7871f357808edaa1fc6ce">git.kernel.org/stable/c/7ef3fd250f84494fb2f7871f357808edaa1fc6ce</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/1034719fdefd26caeec0a44a868bb5a412c2c1a5">git.kernel.org/stable/c/1034719fdefd26caeec0a44a868bb5a412c2c1a5</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://cert-portal.siemens.com/productcert/html/ssa-032379.html">cert-portal.siemens.com/productcert/html/ssa-032379.html</a>	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	<a href="https://cert-portal.siemens.com">cert-portal.siemens.com</a>
<a href="https://git.kernel.org/stable/c/275e37532e8ebe25e8a4069b2d9f955bfd202a46">git.kernel.org/stable/c/275e37532e8ebe25e8a4069b2d9f955bfd202a46</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/ecfd41166b72b67d3bdeb88d224ff445f6163869">git.kernel.org/stable/c/ecfd41166b72b67d3bdeb88d224ff445f6163869</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://lists.debian.org/debian-lts-announce/2025/10/msg00007.html">lists.debian.org/debian-lts-announce/2025/10/msg00007.html</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://lists.debian.org">lists.debian.org</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

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://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

**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)