



ALSA: usb-audio: Validate UAC3 power domain descriptors, too

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

Summary

CVE	CVE-2025-38729
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-09-04 16:15:43 UTC
Updated	2026-05-12 13:17:03 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: ALSA: usb-audio: Validate UAC3 power domain descripto

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from nvd@nist.gov

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

Problem Types: CWE-787

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS: 3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/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 9a2fe9b801f585baccf8352d82839dcd54b300cf 1666207ba0a5973735ef010812536adde6
CNA	Linux	Linux	affected 9a2fe9b801f585baccf8352d82839dcd54b300cf ebc9e06b6ea978a20abf9b87d41afc51b2d
CNA	Linux	Linux	affected 9a2fe9b801f585baccf8352d82839dcd54b300cf f03418bb9d542f44df78eec2eff4ac83c0a8a
CNA	Linux	Linux	affected 9a2fe9b801f585baccf8352d82839dcd54b300cf 40714daf4d0448e1692c78563faf0ed0f9d9
CNA	Linux	Linux	affected 9a2fe9b801f585baccf8352d82839dcd54b300cf 07c8d78dbb5e0ff8b23f7fd69cd1d4e2ba22
CNA	Linux	Linux	affected 9a2fe9b801f585baccf8352d82839dcd54b300cf cd08d390d15b204cac1d3174f5f149a20c5
CNA	Linux	Linux	affected 9a2fe9b801f585baccf8352d82839dcd54b300cf 29b415ec09f5b9d1dfa2423b826725a8c87
CNA	Linux	Linux	affected 9a2fe9b801f585baccf8352d82839dcd54b300cf 452ad54f432675982cc0d6eb6c40a6c86ac
CNA	Linux	Linux	affected 9a2fe9b801f585baccf8352d82839dcd54b300cf d832ccbc301fbd9e5a1d691bdcf461cdb51
CNA	Linux	Linux	affected 4.17
CNA	Linux	Linux	unaffected 4.17 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
lists.debian.org/debian-lts-announce/2025/10/msg00008.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
git.kernel.org/stable/c/40714daf4d0448e1692c78563faf0ed0f9d9b5c7	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/f03418bb9d542f44df78eec2eff4ac83c0a8ac0d	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/1666207ba0a5973735ef010812536adde6174e81	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/cd08d390d15b204cac1d3174f5f149a20c52e61a	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/452ad54f432675982cc0d6eb6c40a6c86ac61dbd	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/d832ccbc301fbd9e5a1d691bdcf461cdb514595f	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/29b415ec09f5b9d1dfa2423b826725a8c8796b9a	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/07c8d78dbb5e0ff8b23f7fd69cd1d4e2ba22b3dc	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/ebc9e06b6ea978a20abf9b87d41afc51b2d745ac	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://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

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