



ALSA: usb-audio: Use correct version for UAC3 header validation

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

Summary

CVE	CVE-2026-23318
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-25 11:16:28 UTC
Updated	2026-04-18 09:16:18 UTC

Description In the Linux kernel, the following vulnerability has been resolved: ALSA: usb-audio: Use correct version for UAC3 header va

Risk And Classification

EPSS: 0.000320000 probability, percentile 0.090980000 (date 2026-04-18)

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 57f8770620e9b51c61089751f0b5ad3dbe376ff2 82a7d0a1b88798de1a609130080ce0c65dd869e9 git
CNA	Linux	Linux	affected 57f8770620e9b51c61089751f0b5ad3dbe376ff2 8307d93e63d5f54ef10412d4db2dd551e920dee4 git
CNA	Linux	Linux	affected 57f8770620e9b51c61089751f0b5ad3dbe376ff2 0dcd1ed96c03459cf14706885c9dd3c1fd8bd29f git
CNA	Linux	Linux	affected 57f8770620e9b51c61089751f0b5ad3dbe376ff2 a0c6ae2ea84528f198bf7fd0117f12fd0cf6d7cc git
CNA	Linux	Linux	affected 57f8770620e9b51c61089751f0b5ad3dbe376ff2 d3904ca40515272681ae61ad6f561c24f190957f git
CNA	Linux	Linux	affected 57f8770620e9b51c61089751f0b5ad3dbe376ff2 1e5753ff4c2e86aa88516f97a224c90a3d0b133e git
CNA	Linux	Linux	affected 57f8770620e9b51c61089751f0b5ad3dbe376ff2 499fd15b00dc91ac95c28f76959dfb5cdcc84d5 git
CNA	Linux	Linux	affected 57f8770620e9b51c61089751f0b5ad3dbe376ff2 54f9d645a5453d0bfece0c465d34aaf072ea99fa git
CNA	Linux	Linux	affected 17821e2fb16752f5d363fb5c3f8aab4df41b9bcc git
CNA	Linux	Linux	affected bf74a46aebb1b5ab5e5f25bafa4ae0a453ba813a git
CNA	Linux	Linux	affected 5.4
CNA	Linux	Linux	unaffected 5.4 semver
CNA	Linux	Linux	unaffected 5.10.253 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.203 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.167 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.130 6.6.* semver

CNA	Linux	Linux	unaffected 6.12.77 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.17 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.7 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/1e5753ff4c2e86aa88516f97a224c90a3d0b133e	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/499ffd15b00dc91ac95c28f76959dfb5cdcc84d5	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/54f9d645a5453d0bfec0c465d34aaf072ea99fa	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/8307d93e63d5f54ef10412d4db2dd551e920dee4	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/0dcd1ed96c03459cf14706885c9dd3c1fd8bd29f	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/82a7d0a1b88798de1a609130080ce0c65dd869e9	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/d3904ca40515272681ae61ad6f561c24f190957f	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/a0c6ae2ea84528f198bf7fd0117f12fd0cf6d7cc	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). 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