



# ALSA: aloop: Fix racy access at PCM trigger

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

## Summary

<b>CVE</b>	CVE-2026-23191
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-02-14 17:15:56 UTC
<b>Updated</b>	2026-04-03 14:16:26 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: ALSA: aloop: Fix racy access at PCM trigger The PCM trigger

## Risk And Classification

**Primary CVSS:** v3.1 7 HIGH from nvd@nist.gov

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

**Problem Types:** CWE-416

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7	HIGH	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:H/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 b1c73fc8e697eb73e23603e465e9af2711ed4183 bad15420050db1803767e58756114800cce91ea4 g
CNA	Linux	Linux	affected b1c73fc8e697eb73e23603e465e9af2711ed4183 5727ccf9d19ca414cb76d9b647883822e2789c2e git
CNA	Linux	Linux	affected b1c73fc8e697eb73e23603e465e9af2711ed4183 826af7fa62e347464b1b4e0ba2fe19a92438084f git
CNA	Linux	Linux	affected 2.6.37
CNA	Linux	Linux	unaffected 2.6.37 semver
CNA	Linux	Linux	unaffected 6.12.70 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.10 6.18.* semver
CNA	Linux	Linux	unaffected 6.19 * original_commit_for_fix

### References

Reference	Source	Link	Tags
git.kernel.org/stable/c/826af7fa62e347464b1b4e0ba2fe19a92438084f	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
git.kernel.org/stable/c/bad15420050db1803767e58756114800cce91ea4	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
git.kernel.org/stable/c/5727ccf9d19ca414cb76d9b647883822e2789c2e	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonic
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)