



# ALSA: ctxfi: Check the error for index mapping

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2026-31777
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-01 15:16:41 UTC
<b>Updated</b>	2026-05-07 02:27:02 UTC
<b>Description</b>	In the Linux kernel, the following vulnerability has been resolved: ALSA: ctxfi: Check the error for index mapping The ctxfi d

## Risk And Classification

**Primary CVSS:** v3.1 5.5 MEDIUM from nvd@nist.gov

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

**EPSS:** 0.000180000 probability, percentile 0.049770000 (date 2026-05-05)

**Problem Types:** NVD-CWE-noinfo

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	7.0	rc1	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	7.0	rc2	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	7.0	rc3	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	7.0	rc4	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	7.0	rc5	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	7.0	rc6	All	All

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 8cc72361481f00253f1e468ade5795427386d593 d4d3b8cbb70a2de247cbfe99bdb232aef9ed59bc git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 8cc72361481f00253f1e468ade5795427386d593 277c6960d4ddb94d16198afd70c92c3d4593d131 gi
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 2.6.31
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 2.6.31 semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.19.12 6.19.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 7.0 * original_commit_for_fix

## References

Reference	Source	Link	Tags
<a href="https://git.kernel.org/stable/c/d4d3b8cbb70a2de247cbfe99bdb232aef9ed59bc">git.kernel.org/stable/c/d4d3b8cbb70a2de247cbfe99bdb232aef9ed59bc</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
<a href="https://git.kernel.org/stable/c/277c6960d4ddb94d16198afd70c92c3d4593d131">git.kernel.org/stable/c/277c6960d4ddb94d16198afd70c92c3d4593d131</a>	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>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical

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)