



# ALSA: firewire-lib: Avoid division by zero in apply\_constraint\_to\_size()

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

## Summary

<b>CVE</b>	CVE-2024-50205
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-11-08 06:15:16 UTC
<b>Updated</b>	2026-05-12 13:16:19 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: ALSA: firewire-lib: Avoid division by zero in apply\_constraint\_to\_size()

## 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

**Problem Types:** CWE-369 | CWE-369 CWE-369 Divide By Zero

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
3.1	ADP	DECLARED	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

## 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	Linux	Linux Kernel	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 826b5de90c0bca4e9de6231da9e1730480621588 d575c
CNA	Linux	Linux	affected 826b5de90c0bca4e9de6231da9e1730480621588 5e43
CNA	Linux	Linux	affected 826b5de90c0bca4e9de6231da9e1730480621588 7d4e
CNA	Linux	Linux	affected 826b5de90c0bca4e9de6231da9e1730480621588 d282
CNA	Linux	Linux	affected 826b5de90c0bca4e9de6231da9e1730480621588 4bdc
CNA	Linux	Linux	affected 826b5de90c0bca4e9de6231da9e1730480621588 3452
CNA	Linux	Linux	affected 826b5de90c0bca4e9de6231da9e1730480621588 72ca
CNA	Linux	Linux	affected 4.20
CNA	Linux	Linux	unaffected 4.20 semver
CNA	Linux	Linux	unaffected 5.4.285 5.4.* semver
CNA	Linux	Linux	unaffected 5.10.229 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.170 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.115 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.59 6.6.* semver
CNA	Linux	Linux	unaffected 6.11.6 6.11.* semver
CNA	Linux	Linux	unaffected 6.12 * original_commit_for_fix
ADP	Siemens	SIMATIC S7-1500 TM MFP - GNU/Linux Subsystem	affected * custom

### References

Reference	Source	Link
git.kernel.org/stable/c/d2826873db70a6719cdd9212a6739f3e6234cfc4	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
lists.debian.org/debian-lts-announce/2025/03/msg00002.html	af854a3a-2127-422b-91ae-364da2661108	<a href="https://lists.debian.org">lists.debian.org</a>
git.kernel.org/stable/c/d575414361630b8b0523912532fcd7c79e43468c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
git.kernel.org/stable/c/72cafe63b35d06b5cfbaf807e90ae657907858da	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>

cert-portal.siemens.com/productcert/html/ssa-265688.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	<a href="https://cert-portal.siemens.com/productcert/html/ssa-265688.html">cert-portal.siemens.cc</a>
<a href="https://git.kernel.org/stable/c/4bdc21506f12b2d432b1f2667e5ff4c75eee58e3">git.kernel.org/stable/c/4bdc21506f12b2d432b1f2667e5ff4c75eee58e3</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/5e431f85c87bbffd93a9830d5a576586f9855291">git.kernel.org/stable/c/5e431f85c87bbffd93a9830d5a576586f9855291</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/3452d39c4704aa12504e4190298c721fb01083c3">git.kernel.org/stable/c/3452d39c4704aa12504e4190298c721fb01083c3</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/2025/01/msg00001.html">lists.debian.org/debian-lts-announce/2025/01/msg00001.html</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://lists.debian.org">lists.debian.org</a>
<a href="https://git.kernel.org/stable/c/7d4eb9e22131ec154e638cbd56629195c9bcbe9a">git.kernel.org/stable/c/7d4eb9e22131ec154e638cbd56629195c9bcbe9a</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.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](https://www.mitre.org/licenses).

**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)