



ALSA: pcm: fix use-after-free on linked stream runtime in snd_pcm_drain()

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

Summary

CVE	CVE-2026-43437
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-08 15:16:56 UTC
Updated	2026-05-11 08:16:14 UTC

Description In the Linux kernel, the following vulnerability has been resolved: ALSA: pcm: fix use-after-free on linked stream runtime in s

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

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

EPSS: 0.000240000 probability, percentile 0.070400000 (date 2026-05-10)

Version	Source	Type	Score	Severity	Vector
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

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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected f2b3614cefb61ee6046a0aaee503ee37f227d310 9baee36e8c5443411c4629afabafaff8a46a23fd git
CNA	Linux	Linux	affected f2b3614cefb61ee6046a0aaee503ee37f227d310 fc71f888994569f87d5bee20b1ac6c9c1e3a7a79 git
CNA	Linux	Linux	affected f2b3614cefb61ee6046a0aaee503ee37f227d310 629cf09464cf98670996ea5c191dc9743e6f3f00 git
CNA	Linux	Linux	affected f2b3614cefb61ee6046a0aaee503ee37f227d310 ae8f8d30d334bad5b1b3cdb1eb8a0b771f55e432 git
CNA	Linux	Linux	affected f2b3614cefb61ee6046a0aaee503ee37f227d310 4a758e9a1f5ed722f83c4dd35f867fe811553bcb git
CNA	Linux	Linux	affected f2b3614cefb61ee6046a0aaee503ee37f227d310 c2f64e05a0587a83ec42dbd6b7a7ded79b2ff694 git
CNA	Linux	Linux	affected f2b3614cefb61ee6046a0aaee503ee37f227d310 9b1dbd69ba6f8f8c69bc7b77c2ce3b9c6ed05ba6 git
CNA	Linux	Linux	affected 3.0
CNA	Linux	Linux	unaffected 3.0 semver
CNA	Linux	Linux	unaffected 5.10.253 5.10.* 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 6.12.78 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.19 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.9 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/629cf09464cf98670996ea5c191dc9743e6f3f00	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/9b1dbd69ba6f8f8c69bc7b77c2ce3b9c6ed05ba6	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/ae8f8d30d334bad5b1b3cdb1eb8a0b771f55e432	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/c2f64e05a0587a83ec42dbd6b7a7ded79b2ff694	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/9baee36e8c5443411c4629afabafaff8a46a23fd	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/4a758e9a1f5ed722f83c4dd35f867fe811553bcb	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/fc71f888994569f87d5bee20b1ac6c9c1e3a7a79	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	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](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)