ALSA: mixer: oss: Add card disconnect checkpoints

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-43126
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-06 12:16:29 UTC
Updated	2026-05-08 17:56:07 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: ALSA: mixer: oss: Add card disconnect checkpoints ALSA

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: 0.000130000 probability, percentile 0.023990000 (date 2026-05-12)

Problem Types: NVD-CWE-noinfo

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

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 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 ae583f113d15fa97e5234133c20d09f8e6214e47 git
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 e6645e625480cdf1079a4265f758d13b70721029 git
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 8c097cf736993454acf3f711a3b376d6c7ad8965 git
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 084d5d44418148662365eced3e126ad1a81ee3e2 git
CNA	Linux	Linux	affected 2.6.12
CNA	Linux	Linux	unaffected 2.6.12 semver
CNA	Linux	Linux	unaffected 6.12.75 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.16 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.6 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/ae583f113d15fa97e5234133c20d09f8e6214e47	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/e6645e625480cdf1079a4265f758d13b70721029	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/084d5d44418148662365eced3e126ad1a81ee3e2	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/8c097cf736993454acf3f711a3b376d6c7ad8965	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report