

CVE-2023-0266

Linux Kernel Use-After-Free Vulnerability

CISA KEV since Mar 30, 2023

Actively exploited

A use after free vulnerability exists in the ALSA PCM package in the Linux Kernel. SNDRV_CTL_IOCTL_ELEM_{READ|WRITE} 32 is missing locks that can be used in a use-after-free that can result in a privilege escalation to gain ring0 access from the system user. We recommend upgrading past commit 56b88b50565cd8b946a2d00b0c83927b7ebb055e

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 7.0 High · NVD	EPSS 0.037 89.6th percentile · FIRST	CISA DEADLINE Apr 20, 2023 KEV since 2023 · listed over a year
---	---------------------------------------	---	---

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.037 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.0	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified**CISA required action:** Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
debian linux	10.0	no fixed version listed	NVD
linux kernel	≥ 4.14 < 4.14.303 ≥ 4.15 < 4.19.270 ≥ 4.20 < 5.4.229 ≥ 5.5 < 5.10.163 ≥ 5.11 < 5.15.88 ≥ 5.16 < 6.1.6	no fixed version listed	NVD

Sources

Vendor guidance	git.kernel.org/pub/scm/linux/kernel/git/stable/stable-queue.git/tree/queue-5.10/alsa-pcm-move-rwsem-lock-inside-snd_ctl_elem_read-to-prevent-uaf.patch?id=72783cf35e6c55bca84c4bb7b776c58152856fd4	NVD	nvd.nist.gov/vuln/detail/CVE-2023-0266
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2023-12345
Current data	evulnable.com/vulnerability-management/cve/CVE-2023-0266		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.