CVE-2014-4655

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

Summary

CVE	CVE-2014-4655
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-07-03 04:22:00 UTC
Updated	2023-11-07 02:20:00 UTC
Description	The snd_ctl_elem_add function in sound/core/control.c in the ALSA control implementation in the Linux kernel before 3.15.2

Risk And Classification

Problem Types: CWE-190

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Suse	Linux Enterprise Server	10	sp4	All	All
Operating System	Suse	Linux Enterprise Server	10	sp4	All	All

References

Reference
[security-announce] SUSE-SU-2015:0812-1: important: Security update for
Red Hat Customer Portal
www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.15.2
Security Advisory SA59777 - Ubuntu update for kernel - Secunia
Linux Kernel Multiple Local Security Bypass Vulnerabilities
kernel/git/torvalds/linux.git - Linux kernel source tree
Google Android Multiple Flaws Let Remote Users Deny Service and Execute Arbitrary Code and Let Applications Obtain Potentially Sensitive
ALSA: control: Fix replacing user controls · torvalds/linux@82262a4 · GitHub

kernel/git/torvalds/linux.git - Linux kernel source tree
USN-2335-1: Linux kernel (OMAP4) vulnerabilities | Ubuntu
Security Advisory SA60564 - Ubuntu update for kernel - Secunia
Security Advisory SA59434 - Linux Kernel ALSA Multiple Vulnerabilities - Secunia
oss-security - Re: CVE Request: Linux kernel ALSA core control API vulnerabilities
About Secunia Research | Flexera
USN-2334-1: Linux kernel vulnerabilities | Ubuntu
Bug 1113445 – CVE-2014-4654 CVE-2014-4655 Kernel: ALSA: control: use-after-free in replacing user controls
CVE Program record
NVD vulnerability detail

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**