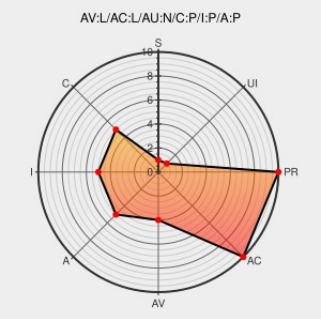
CVE-2014-4656

Published on: 07/02/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:45 PM UTC

CVE-2014-4656

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

Multiple integer overflows in sound/core/control.c in the ALSA control implementation in the Linux kernel before 3.15.2 allow local users to cause a denial of service by leveraging /dev/snd/controlCX access, related to (1) index values in the snd_ctl_add function and (2) numid values in the snd_ctl_remove_numid_conflict function.

CVE-2014-4656 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4.6 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
[security-announce] SUSE-SU-2015:0812-1: important: Security update for	Mailing List, Third Party Advisory, lists.opensuse.org, text/html	SUSE SUSE-SU-2015:0812
Red Hat Customer Portal	Third Party Advisory, web.archive.org, text/html, Inactive Link, Not Archived	REDHAT RHSA-2014:1083
Bug 1113470 – CVE-2014-4656 Kernel: ALSA: control: integer overflow in id.index & id.numid	Issue Tracking, Third Party Advisory, bugzilla.redhat.com, text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1113470

	Release Notes Vendor Advisory www.kernel.org text/plain	CONFIRM www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.15.2
Android Security Bulletin—April 2017 | Android Open Source Project	Third Party Advisory source.android.com text/html	CONFIRM source.android.com/security/bulletin/2017-04-01
Security Advisory SA59777 - Ubuntu update for kernel - Secunia	Third Party Advisory web.archive.org text/html	SECUNIA 59777
Google Android Multiple Flaws Let Users Deny Service, Obtain Potentially Sensitive Information, and Gain Elevated Privileges and Let Remote Users Execute Arbitrary Code - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTRACK 1038201
ALSA: control: Handle numid overflow · torvalds/linux@ac902c1 · GitHub	Patch Third Party Advisory github.com text/html	CONFIRM github.com/torvalds/linux/commit/ac902c112d90a89e59916f751c2745f4dbdbb4bd
kernel/git/torvalds/linux.git - Linux kernel source tree	Patch Vendor Advisory git.kernel.org text/html	CONFIRM git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=ac902c112d90a89e59916f751c2745f4dbdbb4bd
kernel/git/torvalds/linux.git - Linux kernel source tree	Patch Vendor Advisory git.kernel.org text/html	CONFIRM git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=883a1d49f0d77d30012f114b2e19fc141beb3e8e
USN-2335-1: Linux kernel (OMAP4) vulnerabilities | Ubuntu	Third Party Advisory www.ubuntu.com text/html	UBUNTU USN-2335-1
Security Advisory SA60564 - Ubuntu update for kernel - Secunia	Third Party Advisory web.archive.org text/html	SECUNIA 60564
Security Advisory SA59434 - Linux Kernel ALSA Multiple Vulnerabilities - Secunia	Third Party Advisory web.archive.org text/html	SECUNIA 59434
oss-security - Re: CVE Request: Linux kernel ALSA core control API vulnerabilities	Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20140626 Re: CVE Request: Linux kernel ALSA core control API vulnerabilities
Red Hat Customer Portal	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2015:0087
About Secunia Research | Flexera	Third Party Advisory web.archive.org text/html	SECUNIA 60545
USN-2334-1: Linux kernel vulnerabilities | Ubuntu	Third Party Advisory www.ubuntu.com text/html	UBUNTU USN-2334-1

ALSA: control: Make sure that id->index does not overflow · torvalds/linux@883a1d4 · GitHub	Patch Third Party Advisory github.com text/html	CONFIRM github.com/torvalds/linux/commit/883a1d49f0d77d30012f114b2e19fc141beb3e8e

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Eus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Eus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All

Operating System	Suse	Linux Enterprise Server	10	sp4	All	All
Operating System	Suse	Linux Enterprise Server	10	sp4	All	All

cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:esm:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:esm:*:*:*:

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_desktop:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_desktop:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_eus:6.6:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_eus:6.6:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_aus:6.6:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_aus:6.6:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_tus:6.6:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_tus:6.6:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_workstation:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_workstation:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_server:10:sp4:*:*:ltss:*:*:*:

cpe:2.3:o:suse:linux_enterprise_server:10:sp4:*:*:ltss:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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