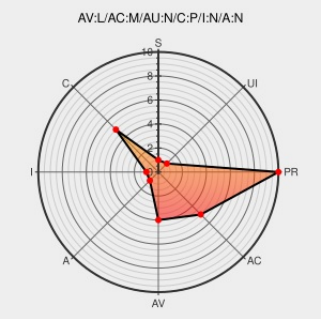
CVE-2014-4652

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

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

CVE-2014-4652

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



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

Race condition in the tlv handler functionality in the snd_ctl_elem_user_tlv function in sound/core/control.c in the ALSA control implementation in the Linux kernel before 3.15.2 allows local users to obtain sensitive information from kernel memory by leveraging /dev/snd/controlCX access.

CVE-2014-4652 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 1.9 - LOW

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

CVE References

Description	Tags	Link
ALSA: control: Protect user controls against concurrent access · torvalds/linux@07f4d9d · GitHub	Patch, Third Party Advisory, github.com, text/html	CONFIRM github.com/torvalds/linux/commit/07f4d9d74a04aa7c72c5dae0ef97565f28f17b92
[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

	Release Notes Vendor Advisory www.kernel.org text/plain	CONFIRM www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.15.2
Security Advisory SA59777 - Ubuntu update for kernel - Secunia	Third Party Advisory web.archive.org text/html	SECUNIA 59777
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=07f4d9d74a04aa7c72c5dae0ef97565f28f17b92
Bug 1113406 – CVE-2014-4652 Kernel: ALSA: control: protect user controls against races & memory disclosure	Issue Tracking Third Party Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1113406
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
About Secunia Research | Flexera	Third Party Advisory web.archive.org text/html	SECUNIA 60545
Red Hat Customer Portal	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2015:1272
USN-2334-1: Linux kernel vulnerabilities | Ubuntu	Third Party Advisory www.ubuntu.com text/html	UBUNTU USN-2334-1
IBM X-Force Exchange	Third Party Advisory VDB Entry exchange.xforce.ibmcloud.com text/html	XF linux-kernel-cve20144652-info-disc(94412)

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 Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	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_server:6.0:*:*:*:*:*:*:*:

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

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→