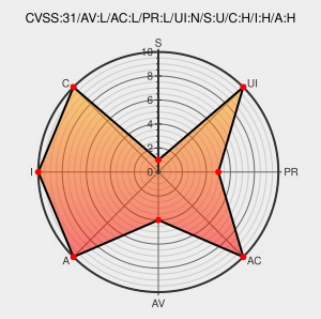
CVE-2014-9904

Published on: 06/27/2016 12:00:00 AM UTC

Last Modified on: 01/17/2023 09:42:00 PM UTC

CVE-2014-9904

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



Certain versions of Debian Linux from Debian contain the following vulnerability:

The snd_compress_check_input function in sound/core/compress_offload.c in the ALSA subsystem in the Linux kernel before 3.17 does not properly check for an integer overflow, which allows local users to cause a denial of service (insufficient memory allocation) or possibly have unspecified other impact via a crafted SNDRV_COMPRESS_SET_PARAMS ioctl call.

CVE-2014-9904 has been assigned by security@android.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 7.2 - HIGH

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

CVE References

Description	Tags	Link
[security-announce] SUSE-SU-2016:1937-1: important:	Third Party Advisory lists.opensuse.org	SUSE SUSE-SU-2016:1937

Security update for	text/html	
ALSA: compress: fix an integer overflow check · torvalds/linux@6217e5e · GitHub	Patch Vendor Advisory github.com text/html	CONFIRM github.com/torvalds/linux/commit/6217e5ede23285ddfee10d2e4ba0cc2d4c046205
Linux Kernel ALSA snd_compr_allocate_buffer() Integer Overflow Lets Local Users Cause Denial of Service Conditions on the Target System - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1036189
Debian -- Security Information -- DSA-3616-1 linux	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-3616
Linux Kernel CVE-2014-9904 Incomplete Fix Local Integer Overflow Vulnerability	cve.report (archive) text/html	BID 91510
kernel/git/torvalds/linux.git - Linux kernel source tree	Patch Vendor Advisory git.kernel.org text/html	CONFIRM git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=6217e5ede23285ddfee10d2e4ba0cc2d4c046205
[security-announce] SUSE-SU-2016:2105-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:2105
[security-announce] openSUSE-SU-2016:2184-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2016:2184

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Novell	Suse Linux Enterprise Real Time Extension	12	sp1	All	All

Operating System	Novell	Suse Linux Enterprise Real Time Extension	12	sp1	All	All

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

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

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

cpe:2.3:o:novell:suse_linux_enterprise_real_time_extension:12:sp1:*:*:*:*:*:*:

cpe:2.3:o:novell:suse_linux_enterprise_real_time_extension:12:sp1:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→