CVE-2017-15265

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

Summary

CVE	CVE-2017-15265
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-10-16 18:29:00 UTC
Updated	2023-06-21 20:59:00 UTC
Description	Race condition in the ALSA subsystem in the Linux kernel before 4.13.8 allows local users to cause a denial of service (use

Risk And Classification

Problem Types: CWE-362 | CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference	Sourc
ALSA: seq: Fix use-after-free at creating a port · torvalds/linux@7110599 · GitHub	CONF
USN-3698-1: Linux kernel vulnerabilities | Ubuntu security notices	UBUN
Bug 1062520 – VUL-1: CVE-2017-15265: kernel: Use-after-free in /dev/snd/seq	CONF
oss-security - Linux kernel: alsa: use-after-free in /dev/snd/seq CVE-2017-15265	MLIS
Linux kernel CVE-2017-15265 Use After Free Local Denial of Service Vulnerability	BID
www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.13.8	CONF
USN-3698-2: Linux kernel (Trusty HWE) vulnerabilities | Ubuntu security notices	UBUN
Oracle Critical Patch Update Advisory - July 2020	MISC
Red Hat Customer Portal	REDH
Red Hat Customer Portal	REDH
[SECURITY] [DLA 1200-1] linux security update	MLIS
Red Hat Customer Portal	REDH

Linux Kernel Use-After-Free Memory Error in ALSA Sequencer Interface Lets Local Users Gain Elevated Privileges - SecurityTracker	SECT
DCIM Support	CONF
kernel/git/torvalds/linux.git - Linux kernel source tree	CONF
Red Hat Customer Portal	REDH
Red Hat Customer Portal	REDH
Red Hat Customer Portal	REDH
Android Security Bulletin—February 2018 | Android Open Source Project	CONF
Red Hat Customer Portal	REDH
[alsa-devel] [PATCH] ALSA: seq: Fix use-after-free at creating a port	MLIS
Oracle Critical Patch Update Advisory - April 2019	MISC
CVE Program record	CVE.(
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.