CVE-2017-15115

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

Summary

CVE	CVE-2017-15115
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-11-15 21:29:00 UTC
Updated	2023-01-19 15:46:00 UTC
Description	The sctp_do_peeloff function in net/sctp/socket.c in the Linux kernel before 4.14 does not check whether the intended netns

Risk And Classification

Problem Types: CWE-416

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	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	17.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	17.10	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	7.0	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	11	sp4	All	All
Operating System	Suse	Linux Enterprise Server	11	sp4	All	All

References

Reference	Source	Link	Tags

[net] sctp: do not peel off an assoc from one netns to another one - Patchwork	CONFIRM	patchwork.ozlabs.org	Issue
sctp: do not peel off an assoc from one netns to another one · torvalds/linux@df80cd9 · GitHub	CONFIRM	github.com	Issue
USN-3581-3: Linux kernel (Raspberry Pi 2) vulnerabilities | Ubuntu security notices | Ubuntu	UBUNTU	usn.ubuntu.com	Third
USN-3582-2: Linux kernel (Xenial HWE) vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com	Third
Bug 1513345 – CVE-2017-15115 kernel: use-after-free in sctp_cmp_addr_exact	CONFIRM	bugzilla.redhat.com	Issue
oss-sec: CVE-2017-15115: Linux kernel: sctp: use-after-free in sctp_cmp_addr_exact()	CONFIRM	seclists.org	Issue
[SECURITY] [DLA 1200-1] linux security update	MLIST	lists.debian.org	Maili
USN-3582-1: Linux kernel vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com	Third
USN-3581-1: Linux kernel vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com	Third
Pixel / Nexus Security Bulletin—April 2018 | Android Open Source Project	CONFIRM	source.android.com	Third
USN-3583-2: Linux kernel (Trusty HWE) vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com	Third
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.kernel.org	Issue
USN-3583-1: Linux kernel vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com	Third
Linux kernel CVE-2017-15115 Local Denial of Service Vulnerability	BID	www.securityfocus.com	Third
[security-announce] SUSE-SU-2018:0011-1: important: Security update for	SUSE	lists.opensuse.org	Third
USN-3581-2: Linux kernel (HWE) vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com	Third
CVE Program record	CVE.ORG	www.cve.org	canc
NVD vulnerability detail	NVD	nvd.nist.gov	canc

No vendor comments have been submitted for this CVE.

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