CVE-2017-5986

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

Summary

CVE	CVE-2017-5986
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-02-18 21:59:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	Race condition in the sctp_wait_for_sndbuf function in net/sctp/socket.c in the Linux kernel before 4.9.11 allows local users

Risk And Classification

Problem Types: CWE-362 | CWE-617

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
Linux Kernel 'net/sctp/socket.c' Local Denial of Service Vulnerability	BID	www.securityfocus.com
Debian -- Security Information -- DSA-3804-1 linux	DEBIAN	www.debian.org
sctp: avoid BUG_ON on sctp_wait_for_sndbuf · torvalds/linux@2dcab59 · GitHub	CONFIRM	github.com
www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.9.11	CONFIRM	www.kernel.org
Red Hat Customer Portal	REDHAT	access.redhat.com
Bug 1420276 – CVE-2017-5986 kernel: Reachable BUG_ON from userspace in sctp_wait_for_sndbuf	CONFIRM	bugzilla.redhat.com
oss-security - Re: Linux kernel: Reachable BUG_ON from userspace in sctp_wait_for_sndbuf()	MLIST	www.openwall.com
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.kernel.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

378249 Virtuozzo Linux Security Update for kernel-tools-libs (VZLSA-2017:1308)

Free CVE JSON API cve.report/api

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