CVE-2017-5669

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

Summary

CVE	CVE-2017-5669
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-02-24 15:59:00 UTC
Updated	2020-10-09 14:49:00 UTC
Description	The do_shmat function in ipc/shm.c in the Linux kernel through 4.9.12 does not restrict the address calculated by a certain

Risk And Classification

Problem Types: NVD-CWE-noinfo

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	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
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

References

Reference	Source	Link	Ta
Debian -- Security Information -- DSA-3804-1 linux	DEBIAN	www.debian.org	Th
Linux Kernel CVE-2017-5669 Local Security Bypass Vulnerability	BID	www.securityfocus.com	Th
ipc/shm: Fix shmat mmap nil-page protection · torvalds/linux@95e91b8 · GitHub	MISC	github.com	Pa
Linux Kernel do_shmat() Flaw Lets Local Users Bypass Security Restrictions - SecurityTracker	SECTRACK	www.securitytracker.com	Th
USN-3583-2: Linux kernel (Trusty HWE) vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com	Th
192931 – Shmat allows mmap null page protection bypass	MISC	bugzilla.kernel.org	Is

USN-3583-1: Linux kernel vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com	Tl
ipc/shm: Fix shmat mmap nil-page protection · torvalds/linux@e1d35d4 · GitHub	CONFIRM	github.com	P.
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

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