CVE-2015-5707

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

Summary

CVE	CVE-2015-5707
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-10-19 10:59:00 UTC
Updated	2020-06-02 14:57:00 UTC
Description	Integer overflow in the sg_start_req function in drivers/scsi/sg.c in the Linux kernel 2.6.x through 4.x before 4.1 allows local

Risk And Classification

Problem Types: CWE-190

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	15.04	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	Canonical	Ubuntu Linux	15.04	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	7.0	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	Suse	Suse Linux Enterprise Desktop	11	sp3	All	All
Operating System	Suse	Suse Linux Enterprise Desktop	11	sp3	All	All
Operating System	Suse	Suse Linux Enterprise Server	11	sp2	All	All
Operating System	Suse	Suse Linux Enterprise Server	11	sp3	All	All
Operating System	Suse	Suse Linux Enterprise Server	11	sp3	All	All

Operating System	Suse	Suse Linux Enterprise Server	11	sp2	All	All
Operating System	Suse	Suse Linux Enterprise Server	11	sp3	All	All
Operating System	Suse	Suse Linux Enterprise Server	11	sp3	All	All

References

Reference	Source	Link
USN-2738-1: Linux kernel vulnerability | Ubuntu	UBUNTU	www.ubuntu.c
sg_start_req(): use import_iovec() · torvalds/linux@fdc81f4 · GitHub	CONFIRM	github.com
Linux Kernel '/scsi/sg.c' Integer Overflow Vulnerability	BID	www.securityfo
[security-announce] SUSE-SU-2015:2086-1: important: Security update for	SUSE	lists.opensuse
[security-announce] SUSE-SU-2015:2091-1: important: Security update for	SUSE	lists.opensuse
Linux Kernel SCSI Generic Driver Integer Overflow Lets Local Users Obtain Root Privileges - SecurityTracker	SECTRACK	www.securitytr
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.kernel.org
USN-2750-1: Linux kernel (Utopic HWE) vulnerability | Ubuntu	UBUNTU	www.ubuntu.c
USN-2760-1: Linux kernel (OMAP4) vulnerabilities | Ubuntu	UBUNTU	www.ubuntu.c
oss-security - CVE request: Integer overflow in SCSI generic driver in Linux <4.1	MLIST	www.openwall
USN-2759-1: Linux kernel vulnerabilities | Ubuntu	UBUNTU	www.ubuntu.c
[security-announce] SUSE-SU-2015:2090-1: important: Security update for	SUSE	lists.opensuse
Android Security Bulletin—July 2017 | Android Open Source Project	CONFIRM	source.androic
[security-announce] SUSE-SU-2015:2084-1: important: Security update for	SUSE	lists.opensuse
[security-announce] SUSE-SU-2015:1478-1: important: Security update for	SUSE	lists.opensuse
USN-2734-1: Linux kernel vulnerability | Ubuntu	UBUNTU	www.ubuntu.c
USN-2737-1: Linux kernel (Vivid HWE) vulnerability | Ubuntu	UBUNTU	www.ubuntu.c
[security-announce] SUSE-SU-2015:2085-1: important: Security update for	SUSE	lists.opensuse
[security-announce] SUSE-SU-2015:1611-1: important: Security update for	SUSE	lists.opensuse
Debian -- Security Information -- DSA-3329-1 linux	DEBIAN	www.debian.o
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.kernel.org
USN-2733-1: Linux kernel (Trusty HWE) vulnerability | Ubuntu	UBUNTU	www.ubuntu.c
[security-announce] SUSE-SU-2015:1592-1: important: Security update for	SUSE	lists.opensuse
[security-announce] SUSE-SU-2015:2089-1: important: Security update for	SUSE	lists.opensuse
[security-announce] SUSE-SU-2015:2087-1: important: Security update for	SUSE	lists.opensuse
Bug 1250030 – CVE-2015-5707 kernel: number wraparound vulnerability in function start_req()	CONFIRM	bugzilla.redhat
sg_start_req(): make sure that there's not too many elements in iovec · torvalds/linux@451a288 · GitHub	CONFIRM	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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