CVE-2014-5077

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

Summary

CVE	CVE-2014-5077
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-08-01 11:13:00 UTC
Updated	2023-05-19 16:50:00 UTC
Description	The sctp_assoc_update function in net/sctp/associola.c in the Linux kernel through 3.15.8, when SCTP authentication is en

Risk And Classification

Problem Types: CWE-476

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	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Redhat	Enterprise Linux Eus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Eus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	6.5	All	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp3	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp3	All	All
Operating System	Suse	Linux Enterprise Real Time Extension	11	sp3	All	All

Operating System	Suse	Linux Enterprise Real Time Extension	11	sp3	All	All
Operating System	Suse	Linux Enterprise Server	11	sp3	All	All
Operating System	Suse	Linux Enterprise Server	11	sp3	All	All
Operating System	Suse	Linux Enterprise Server	11	sp3	All	All
Operating System	Suse	Linux Enterprise Server	11	sp3	All	All

References

Reference	Source	Link
Security Advisory SA60430 - Linux Kernel NULL Pointer Dereference Vulnerabilities - Secunia	SECUNIA	secur
oss-security - Re: CVE request Linux Kernel: net: SCTP: NULL pointer dereference	MLIST	www.
Red Hat Customer Portal	REDHAT	rhn.re
Linux Kernel SCTP Null Pointer Dereference Lets Remote Users Deny Service - SecurityTracker	SECTRACK	www.
Red Hat Customer Portal	MISC	acces
[security-announce] SUSE-SU-2014:1319-1: important: Security update for	SUSE	lists.o
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.ke
Security Advisory SA59777 - Ubuntu update for kernel - Secunia	SECUNIA	secur
Red Hat Customer Portal	MISC	acces
Security Advisory SA62563 - Red Hat update for kernel - Secunia	SECUNIA	secur
net: sctp: inherit auth_capable on INIT collisions · torvalds/linux@1be9a95 · GitHub	CONFIRM	githul
Red Hat Customer Portal	MISC	acces
USN-2358-1: Linux kernel (Trusty HWE) vulnerabilities | Ubuntu	UBUNTU	www.
Linux Kernel SCTP NULL Pointer Dereference Denial of Service Vulnerability	BID	www.
USN-2335-1: Linux kernel (OMAP4) vulnerabilities | Ubuntu	UBUNTU	www.
[security-announce] SUSE-SU-2014:1316-1: important: Security update for	SUSE	lists.o
1122982 – (CVE-2014-5077) CVE-2014-5077 Kernel: net: SCTP: fix a NULL pointer dereference during INIT collisions	CONFIRM	bugzi
Red Hat Customer Portal	REDHAT	rhn.re
Security Advisory SA60564 - Ubuntu update for kernel - Secunia	SECUNIA	secur
Red Hat Customer Portal	MISC	acces
Red Hat Customer Portal	REDHAT	rhn.re
Red Hat Customer Portal	MISC	acces
USN-2359-1: Linux kernel vulnerabilities | Ubuntu	UBUNTU	www.
access.redhat.com | CVE-2014-5077	MISC	acces
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.ke
About Secunia Research | Flexera	SECUNIA	secur
IBM X-Force Exchange	XF	excha

Security Advisory SA60744 - Red Hat update for kernel - Secunia	SECUNIA	secur
Red Hat Customer Portal	MISC	acces
USN-2334-1: Linux kernel vulnerabilities | Ubuntu	UBUNTU	www.
CVE Program record	CVE.ORG	www.
NVD vulnerability detail	NVD	nvd.n

No vendor comments have been submitted for this CVE.

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