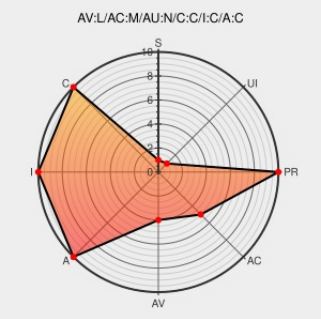
CVE-2013-1828

Published on: 03/22/2013 12:00:00 AM UTC

Last Modified on: 08/11/2023 06:41:00 PM UTC

CVE-2013-1828

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Linux Kernel from Linux contain the following vulnerability:

The sctp_getsockopt_assoc_stats function in net/sctp/socket.c in the Linux kernel before 3.8.4 does not validate a size value before proceeding to a copy_from_user operation, which allows local users to gain privileges via a crafted application that contains an SCTP_GET_ASSOC_STATS getsockopt system call.

CVE-2013-1828 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 6.9 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Linux Kernel 'SCTP_GET_ASSOC_STATS()' - Stack-Based Buffer Overflow	www.exploit-db.com, Proof of Concept, text/x-c	EXPLOIT-DB 24747
JavaScript is not available.	nitter.domain.glass, text/html	MISC twitter.com/grsecurity/statuses/309805924749541376
No Description Provided	Exploit, Patch, git.kernel.org, text/html, Inactive Link, Not Archived	MISC git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git%3Ba=commit%3Bh=726bc6b092da4c093eb74d13c07184b18c1af0f1
oss-security - Re: CVE Request -- Linux kernel: sctp:	www.openwall.com, text/html	MLIST [oss-security] 20130307 Re: CVE Request -- Linux kernel: sctp: SCTP_GET_ASSOC_STATS stack overflow

SCTP_GET_ASSOC_STATS stack overflow		
919315 – (CVE-2013-1828) CVE-2013-1828 kernel: sctp: SCTP_GET_ASSOC_STATS stack buffer overflow	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=919315
	Exploit grsecurity.net text/x-c	MISC grsecurity.net/~spender/sctp.c
	www.kernel.org text/plain	CONFIRM www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.8.4
net/sctp: Validate parameter size for SCTP_GET_ASSOC_STATS · torvalds/linux@726bc6b · GitHub	Exploit Patch github.com text/html	CONFIRM github.com/torvalds/linux/commit/726bc6b092da4c093eb74d13c07184b18c1af

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	3.8.0	All	All	All
Operating System	Linux	Linux Kernel	3.8.1	All	All	All
Operating System	Linux	Linux Kernel	3.8.2	All	All	All
Operating System	Linux	Linux Kernel	3.8.0	All	All	All
Operating System	Linux	Linux Kernel	3.8.1	All	All	All
Operating System	Linux	Linux Kernel	3.8.2	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.8.0:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.8.1:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.8.2:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.8.0:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.8.1:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.8.2:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→