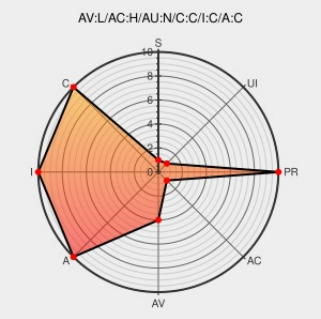
CVE-2013-1826

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

Last Modified on: 02/13/2023 12:27:00 AM UTC

CVE-2013-1826

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



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

The xfrm_state_netlink function in net/xfrm/xfrm_user.c in the Linux kernel before 3.5.7 does not properly handle error conditions in dump_one_state function calls, which allows local users to gain privileges or cause a denial of service (NULL pointer dereference and system crash) by leveraging the CAP_NET_ADMIN capability.

CVE-2013-1826 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 6.2 - MEDIUM

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

CVE References

Description	Tags	Link
xfrm_user: return error pointer instead of NULL · torvalds/linux@864745d · GitHub	github.com text/html	CONFIRM github.com/torvalds/linux/commit/864745d291b5ba80ea0bd0edcbe67273de368836
kernel/git/torvalds/linux.git - Linux kernel source tree	web.archive.org text/html Inactive Link Not Archived	MISC git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git%3Ba=commit%3Bh=864745d291b5ba80ea0bd0edcbe67273de368836
USN-1829-1: Linux kernel (EC2) vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-1829-1
Red Hat Customer Portal	web.archive.org text/html	REDHAT RHSA-2013:0744

	Inactive Link Not Archived	
Bug 919384 – CVE-2013-1826 Kernel: xfrm_user: return error pointer instead of NULL	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=919384
oss-security - Re: CVE Requests (maybe): Linux kernel: various info leaks, some NULL ptr derefs	www.openwall.com text/html	MLIST [oss-security] 20130307 Re: CVE Requests (maybe): Linux kernel: various info leaks, some NULL ptr derefs
	www.kernel.org text/plain	CONFIRM www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.5.7

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	3.5.1	All	All	All
Operating System	Linux	Linux Kernel	3.5.2	All	All	All
Operating System	Linux	Linux Kernel	3.5.3	All	All	All
Operating System	Linux	Linux Kernel	3.5.4	All	All	All
Operating System	Linux	Linux Kernel	3.5.5	All	All	All
Operating System	Linux	Linux Kernel	3.5.1	All	All	All
Operating System	Linux	Linux Kernel	3.5.2	All	All	All
Operating System	Linux	Linux Kernel	3.5.3	All	All	All
Operating System	Linux	Linux Kernel	3.5.4	All	All	All
Operating System	Linux	Linux Kernel	3.5.5	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

cpe:2.3:o:linux:linux_kernel:3.5.1:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.5.2:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.5.3:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.5.4:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.5.5:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.5.1:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.5.2:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.5.3:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.5.4:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.5.5:*:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→