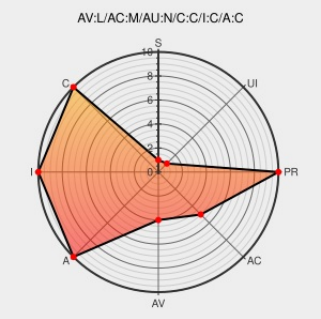
CVE-2009-1897

Published on: 07/20/2009 12:00:00 AM UTC

Last Modified on: 02/13/2023 02:20:00 AM UTC

CVE-2009-1897

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



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

The tun_chr_poll function in drivers/net/tun.c in the tun subsystem in the Linux kernel 2.6.30 and 2.6.30.1, when the -fno-delete-null-pointer-checks gcc option is omitted, allows local users to gain privileges via vectors involving a NULL pointer dereference and an mmap of /dev/net/tun, a different vulnerability than CVE-2009-1894.

CVE-2009-1897 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
No Description Provided	web.archive.org, text/html, Inactive Link, Not Archived	FULLDISC 20090716 Re: Linux 2.6.30+/SELinux/RHEL5 test kernel 0day, exploiting the unexploitable
InfoSec Handlers Diary Blog	Exploit, isc.sans.org, text/html	MISC isc.sans.org/diary.html?storyid=6820
404 Not Found	Patch, grsecurity.net, application/gzip, Inactive Link, Not Archived	MISC grsecurity.net/~spender/cheddar_bay.tgz
Bug 512284 – CVE-2009-1897 kernel: tun/tap: Fix	bugzilla.redhat.com, text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=512284

crashes if open() /dev/net/tun and then poll() it		
Linux Kernel "tun_char_poll()" NULL Pointer Dereference - Secunia Advisories - Vulnerability Information - Secunia.com	Vendor Advisory web.archive.org text/html	SECUNIA 35839
oss-security - Linux 2.6.30+/SELinux/RHEL5 test kernel 0day, exploiting the unexploitable	www.openwall.com text/html	MLIST [oss-security] 20090717 Linux 2.6.30+/SELinux/RHEL5 test kernel 0day, exploiting the unexploitable
Gmane -- Mail To News And Back Again	web.archive.org text/html Inactive Link Not Archived	MLIST [netdev] 20090409 Oops in tun: bisected to Limit amount of queued packets per device
kernel/git/torvalds/linux.git - Linux kernel source tree	Exploit Patch Vendor Advisory 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=3c8a9c63d5fd738c261bd0ceece04d9c8357ca13
Security flaws caused by compiler optimizations	www.redhat.com text/html	MISC www.redhat.com/en/blog/security-flaws-caused-compiler-optimizations
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF linux-kernel-tunchrpoll-code-execution(51803)
LKML: Mariusz Kozlowski: Re: PROBLEM: tun/tap crashes if open() /dev/net/tun and then poll() it.	Exploit lkml.org text/xml	MLIST [linux-kernel] 20090706 Re: PROBLEM: tun/tap crashes if open() /dev/net/tun and then poll() it.
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Patch Vendor Advisory www.vupen.com text/html	VUPEN ADV-2009-1925
No Description Provided	web.archive.org text/html Inactive Link Not Archived	FULLDISC 20090716 Linux 2.6.30+/SELinux/RHEL5 test kernel 0day, exploiting the unexploitable

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	2.6.30	All	All	All
Operating System	Linux	Linux Kernel	2.6.30	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.30	rc2	All	All

Operating System	Linux	Linux Kernel	2.6.30	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.30	rc4	x86_32	All
Operating System	Linux	Linux Kernel	2.6.30	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.30	rc6	All	All
Operating System	Linux	Linux Kernel	2.6.30	rc7-git6	All	All
Operating System	Linux	Linux Kernel	2.6.30.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.30	All	All	All
Operating System	Linux	Linux Kernel	2.6.30	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.30	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.30	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.30	rc4	x86_32	All
Operating System	Linux	Linux Kernel	2.6.30	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.30	rc6	All	All
Operating System	Linux	Linux Kernel	2.6.30	rc7-git6	All	All
Operating System	Linux	Linux Kernel	2.6.30.1	All	All	All

cpe:2.3:o:linux:linux_kernel:2.6.30:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.30:rc1:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.30:rc2:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.30:rc3:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.30:rc4:x86_32:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.30:rc5:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.30:rc6:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.30:rc7-git6:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.30.1:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.30:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.30:rc1:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.30:rc2:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.30:rc3:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.30:rc4:x86_32:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.30:rc5:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.30:rc6:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.30:rc7-git6:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.30.1:*:*:*:*:*:*:*:

← Previous ID

Next ID→