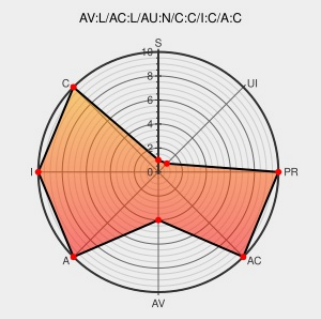
CVE-2005-1264

Published on: 05/17/2005 12:00:00 AM UTC

Last Modified on: 02/13/2023 01:09:25 AM UTC

CVE-2005-1264

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



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

Raw character devices (raw.c) in the Linux kernel 2.6.x call the wrong function before passing an ioctl to the block device, which crosses security boundaries by making kernel address space accessible from user space, a similar vulnerability to CVE-2005-1589.

CVE-2005-1264 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 7.2 - HIGH

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

CVE References

Description	Tags	Link
Neohapsis Archives - VulnWatch - #0046 - Re: [VulnWatch] Linux kernel pktcdvd and rawdevice ioctl break user space limit vulnerability	web.archive.org text/html Inactive Link Not Archived	VULNWATCH 20050517 Re: Linux kernel pktcdvd and rawdevice ioctl break user space limit vulnerability
Webmail : Solution de messagerie professionnelle - OVHcloud-OVH	www.vupen.com text/html	VUPEN ADV-2005-0557
Multiple Linux Kernel IOCTL Handlers Local Memory Corruption Vulnerabilities	cve.report (archive) text/html	BID 13651
SecurityFocus	www.securityfocus.com text/html	FEDORA FLSA:157459-3
Support	www.redhat.com text/html	REDHAT RHSA-2005:420
'[PATCH] Fix root hole in raw device' - MARC	marc.info	MLIST [linux-kernel] 20050517 [PATCH]

	text/x-diff	Fix root hole in raw device
Neohapsis Archives - VulnWatch - #0045 - [VulnWatch] Linux kernel pktcdvd and rawdevice ioctl break user space limit vulnerability	Exploit Patch Vendor Advisory web.archive.org text/html Inactive Link Not Archived	VULNWATCH 20050516 Linux kernel pktcdvd and rawdevice ioctl break user space limit vulnerability
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:10264
	kernel.org text/plain	CONFIRM kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.11.10

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	2.6.0	All	All	All
Operating System	Linux	Linux Kernel	2.6.0	test1	All	All
Operating System	Linux	Linux Kernel	2.6.0	test10	All	All
Operating System	Linux	Linux Kernel	2.6.0	test11	All	All
Operating System	Linux	Linux Kernel	2.6.0	test2	All	All
Operating System	Linux	Linux Kernel	2.6.0	test3	All	All
Operating System	Linux	Linux Kernel	2.6.0	test4	All	All
Operating System	Linux	Linux Kernel	2.6.0	test5	All	All
Operating System	Linux	Linux Kernel	2.6.0	test6	All	All
Operating System	Linux	Linux Kernel	2.6.0	test7	All	All
Operating System	Linux	Linux Kernel	2.6.0	test8	All	All
Operating System	Linux	Linux Kernel	2.6.0	test9	All	All
Operating System	Linux	Linux Kernel	2.6.1	All	All	All

System						
Operating System	Linux	Linux Kernel	2.6.1	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.1	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.6	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.7	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.8	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.8	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.8	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.9	2.6.20	All	All
Operating System	Linux	Linux Kernel	2.6_test9_cvs	All	All	All
Operating System	Linux	Linux Kernel	2.6.0	All	All	All
Operating System	Linux	Linux Kernel	2.6.0	test1	All	All
Operating System	Linux	Linux Kernel	2.6.0	test10	All	All
Operating System	Linux	Linux Kernel	2.6.0	test11	All	All
Operating System	Linux	Linux Kernel	2.6.0	test2	All	All
Operating System	Linux	Linux Kernel	2.6.0	test3	All	All
Operating	Linux	Linux Kernel	2.6.0	test4	All	All

System						
Operating System	Linux	Linux Kernel	2.6.0	test5	All	All
Operating System	Linux	Linux Kernel	2.6.0	test6	All	All
Operating System	Linux	Linux Kernel	2.6.0	test7	All	All
Operating System	Linux	Linux Kernel	2.6.0	test8	All	All
Operating System	Linux	Linux Kernel	2.6.0	test9	All	All
Operating System	Linux	Linux Kernel	2.6.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.1	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.1	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.6	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.7	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.8	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.8	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.8	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.9	2.6.20	All	All
Operating System	Linux	Linux Kernel	2.6_test9_cvs	All	All	All

cpe:2.3:o:linux:linux_kernel:2.6.0:*:*:*:*:*:*:*

cpe:2.3:o:linux:linux_kernel:2.6.0:test1:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.0:test10:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.0:test11:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.0:test2:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.0:test3:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.0:test4:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.0:test5:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.0:test6:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.0:test7:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.0:test8:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.0:test9:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.1:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.1:rc1:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.1:rc2:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.2:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.3:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.4:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.5:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.6:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.6:rc1:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.7:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.7:rc1:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.8:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.8:rc1:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.8:rc2:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.8:rc3:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.9:2.6.20:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6_test9_cvs:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.0:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.0:test1:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.0:test10:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.0:test11:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.0:test2:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.0:test3:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.0:test4:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.0:test5:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.0:test6:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.0:test7:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.0:test8:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.0:test9:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.1:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.1:rc1:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.1:rc2:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.2:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.3:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.4:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.5:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.6:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.6:rc1:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.7:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.7:rc1:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.8:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.8:rc1:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.8:rc2:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.8:rc3:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.9:2.6.20:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6_test9_cvs:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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