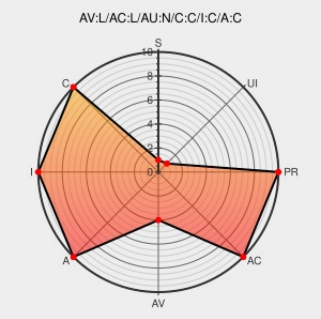
# CVE-2005-1589

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

Last Modified on: 03/23/2021 11:27:25 PM UTC

## CVE-2005-1589

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




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

The pkt_ioctl function in the pktcdvd block device ioctl handler (pktcdvd.c) in Linux kernel 2.6.12-rc4 and earlier calls the wrong function before passing an ioctl to the block device, which crosses security boundaries by making kernel address space accessible from user space and allows local users to cause a denial of service and possibly execute arbitrary code, a similar vulnerability to CVE-2005-1264.

CVE-2005-1589 has been assigned by cve@mitre.org 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 |
| Advisories - Mandriva Linux | www.mandriva.com, text/html | MANDRAKE MDKSA-2005:219 |
| '[PATCH] Fix root hole in pktcdvd' - MARC | marc.info, text/x-diff | MLIST [linux-kernel] 20050517 [PATCH] Fix root hole in pktcdvd |
| Multiple Linux Kernel IOCTL Handlers Local Memory Corruption | cve.report (archive) | BID 13651 |

| | | |
|---|---|---|
| Vulnerabilities | text/html | |
| Neohapsis Archives - VulnWatch - #0045 - [VulnWatch] Linux kernel pktcdvd and rawdevice ioctl break user space limit vulnerability | Exploit<br>Patch<br>Vendor Advisory<br>web.archive.org<br>text/html<br>Inactive Link Not Archived | VULNWATCH 20050516 Linux kernel pktcdvd and rawdevice ioctl break user space limit vulnerability |
| Neohapsis Archives - VulnWatch - #0047 - [VulnWatch] Linux kernel pktcdvd ioctl break user space limit vulnerability [corrected] | web.archive.org<br>text/html<br>Inactive Link Not Archived | VULNWATCH 20050517 Linux kernel pktcdvd ioctl break user space limit vulnerability [corrected] |
| | kernel.org<br>text/plain | CONFIRM kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.11.10 |
| Secunia - Advisories - Mandriva update for kernel | web.archive.org<br>text/html | SECUNIA 17826 |

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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 | rc4 | All | All |

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→