

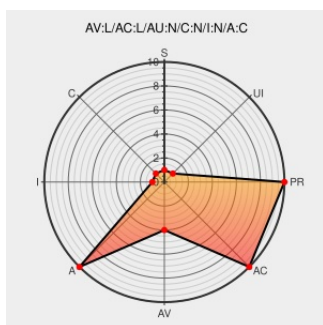


CVE-2004-2660

Published on: 12/31/2004 05:00:00 AM UTC

Last Modified on: 11/07/2023 01:57:00 AM UTC

CVE-2004-2660

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Linux Kernel](#) from [Linux](#) contain the following vulnerability:

Memory leak in direct-io.c in Linux kernel 2.6.x before 2.6.10 allows local users to cause a denial of service (memory consumption) via certain O_DIRECT (direct IO) write requests.

CVE-2004-2660 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.9 - MEDIUM**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

Debian update for kernel-source-2.6.8 - Advisories - Secunia

[web.archive.org](#)
[text/html](#)

[X](#) SECUNIA 22093

No Description Provided

[linux.bkbits.net](#)

[CONFIRM](#) [linux.bkbits.net:8080/linux-2.6/cset@4182a613oVsK0-8eCWpyYFrUf8rhLA](#)

Inactive Link Not Archived

Red Hat update for kernel - Advisories - Secunia

[web.archive.org](#)
[text/html](#)

[X](#) SECUNIA 21605

Linux Kernel Direct-IO.C Local Denial of Service Vulnerability

[cve.report \(archive\)](#)
[text/html](#)

[BID](#) 19665

[rhn.redhat.com](#) | Red Hat Support

[www.redhat.com](#)
[text/html](#)

[REDHAT](#) RHSA-2006:0617

ASA-2006-203 (RHSA-2006-0617)

[support.avaya.com](#)

[CONFIRM](#)

[text/html](#)support.avaya.com/elmodocs2/security/ASA-2006-203.htm

Debian -- Security Information -- DSA-1184-2 kernel-source-2.6.8

www.debian.org
[Deprecated Link](#)
[text/html](#) [DEBIAN DSA-1184](#)

Repository / Oval Repository

oval.cisecurity.org
[text/html](#) [OVAL oval.org/mitre/oval:def:10165](https://oval.org/mitre/oval:def:10165)

Avaya Products Linux Kernel Multiple Vulnerabilities - Advisories - Secunia

web.archive.org
[text/html](#) [SECUNIA 22174](#)[Patch](#)
www.kernel.org
[text/plain](#) [CONFIRM](#)
www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.10

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	2.6.0	All	All	All
Operating System	Linux	Linux Kernel	2.6.0	All	64-bit_x86	All
Operating System	Linux	Linux Kernel	2.6.0	All	itanium_ia64_montecito	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	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	2.6.1	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.2	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.2	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.2	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.3	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.3	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.3	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.3	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.4	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.4	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.4	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.5	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.5	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.5	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.6	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	2.6.6	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.6	rc3	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	2.6.7	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.7	rc3	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	2.6.8	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.8.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	386	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	686	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	686_smp	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	amd64	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	amd64_k8	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	amd64_k8_smp	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	amd64_xeon	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	k7	All

Operating System	Linux	Linux Kernel	2.6.8.1.5	All	k7_smp	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	power3	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	power3_smp	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	power4	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	power4_smp	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	powerpc	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	powerpc_smp	All
Operating System	Linux	Linux Kernel	2.6.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.9	2.6.20	All	All
Operating System	Linux	Linux Kernel	2.6.9	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.9	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.9	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.9	rc4	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	All	64-bit_x86	All
Operating System	Linux	Linux Kernel	2.6.0	All	itanium_ia64_montecito	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
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	2.6.1	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.2	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.2	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.2	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.3	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.3	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.3	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.3	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.4	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.4	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.4	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.5	All	All	All

Operating System	Linux	Linux Kernel	2.6.5	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.5	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.5	rc3	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	2.6.6	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.6	rc3	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	2.6.7	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.7	rc3	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	2.6.8	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.8.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	386	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	686	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	686_smp	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	amd64	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	amd64_k8	All

Operating System	Linux	Linux Kernel	2.6.8.1.5	All	amd64_k8_smp	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	amd64_xeon	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	k7	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	k7_smp	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	power3	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	power3_smp	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	power4	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	power4_smp	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	powerpc	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	powerpc_smp	All
Operating System	Linux	Linux Kernel	2.6.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.9	2.6.20	All	All
Operating System	Linux	Linux Kernel	2.6.9	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.9	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.9	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.9	rc4	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:*:64-bit_x86:*****:*						
cpe:2.3:o:linux:linux_kernel:2.6.0:*:itanium_ia64_montecito:*****:*						
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:2.6.1:rc3:~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.2:~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.2:rc1:~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.2:rc2:~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.2:rc3:~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.3:~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.3:rc1:~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.3:rc2:~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.3:rc3:~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.3:rc4:~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.4:~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.4:rc1:~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.4:rc2:~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.4:rc3:~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.5:~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.5:rc1:~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.5:rc2:~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.5:rc3:~::~~::~~::~~::~~::~~:::
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:2.6.6:rc2:~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.6:rc3:~::~~::~~::~~::~~:::
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:2.6.7:rc2:~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.7:rc3:~::~~::~~::~~::~~:::
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:2.6.8:rc4:~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.8.1:~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5:~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:386:~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:686:~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:686_smp:~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:amd64:~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:amd64_k8:~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:amd64_k8_smp:~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:amd64_xeon:~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:k7:~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:k7_smp:~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:power3:~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:power3_smp:~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:power4:~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:power4_smp:~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:powerpc:~::~~::~~:::

cpe:2.3:o:linux:linux_kernel:2.6.8.1.5:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.9:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.9:2.6.20:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.9:rc1:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.9:rc2:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.9:rc3:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.9:rc4:*:*:*:*:*:
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:*:64-bit_x86:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.0:*:itanium_ia64_montecito:*:*:*:*:
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:2.6.1:rc3:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.2:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.2:rc1:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.2:rc2:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.2:rc3:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.3:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.3:rc1:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.3:rc2:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.3:rc3:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.3:rc4:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.4:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.4:rc1:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.4:rc2:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.4:rc3:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.5:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.5:rc1:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.5:rc2:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.5:rc3:*:*:*:*:
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:2.6.6:rc2:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.6:rc3:*:*:*:*:
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:2.6.7:rc2:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.7:rc3:*:*:*:*:
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:2.6.8:rc4:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.8.1:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.8.1.5:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:386:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:686:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:686_smp:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:amd64:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:amd64_k8:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:amd64_k8_smp:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:amd64_xeon:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:k7:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:k7_smp:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:power3:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:power3_smp:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:power4:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:power4_smp:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:powerpc:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:powerpc_smp:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.9:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.9:2.6.20:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.9:rc1:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.9:rc2:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.9:rc3:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.9:rc4:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6_test9_cvs:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)