

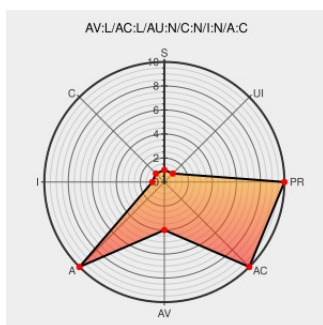


CVE-2006-1525

Published on: 04/19/2006 12:00:00 AM UTC

Last Modified on: 02/13/2023 02:10:35 AM UTC

CVE-2006-1525

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

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

ip_route_input in Linux kernel 2.6 before 2.6.16.8 allows local users to cause a denial of service (panic) via a request for a route for a multicast IP address, which triggers a null dereference.

CVE-2006-1525 has been assigned by secalert@redhat.com 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

Vendor Advisory
web.archive.org
text/html

SECUNIA 20914

Webmail - OVH

Vendor Advisory
www.vupen.com
text/html

VUPEN ADV-2006-2554

Linux Kernel "ip_route_input()" Denial of Service
Vulnerability - Advisories - Secunia

Patch
Vendor Advisory
web.archive.org
text/html

SECUNIA 19709

LWN: Fedora alert FEDORA-2006-423 (kernel)

lwn.net
text/html

FEDORA FEDORA-2006-423

Webmail : Solution de messagerie professionnelle -

Vendor Advisory

VUPEN ADV-2006-1475

OVHcloud- OVH	www.vupen.com text/html	
Red Hat update for kernel - Advisories - Secunia	Vendor Advisory web.archive.org text/html	 SECUNIA 20237
Avaya Products Linux Kernel Multiple Vulnerabilities - Advisories - Secunia	Vendor Advisory web.archive.org text/html	 SECUNIA 21745
Debian -- Security Information -- DSA-1097-1 kernel-source-2.4.27	www.debian.org Deprecated Link text/html	 DEBIAN DSA-1097
Fedora update for kernel - Advisories - Secunia	Vendor Advisory web.archive.org text/html	 SECUNIA 19735
USN-281-1: Linux kernel vulnerabilities Ubuntu security notices	usn.ubuntu.com text/html	 UBUNTU USN-281-1
Mandriva update for kernel - Advisories - Secunia	Vendor Advisory web.archive.org text/html	 SECUNIA 20157
Secunia - Advisories - Ubuntu update for kernel	Vendor Advisory web.archive.org text/html	 SECUNIA 19955
189346 – CVE-2006-1525 ip_route_input() panic	bugzilla.redhat.com text/html	 CONFIRM bugzilla.redhat.com/bugzilla/show_bug.cgi?id=189346
Debian update for kernel-source-2.4.27 - Advisories - Secunia	Vendor Advisory web.archive.org text/html	 SECUNIA 20671
rhn.redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2006:0493
Debian -- Security Information -- DSA-1103-1 kernel-source-2.6.8	www.debian.org Deprecated Link text/html	 DEBIAN DSA-1103
Security Announcement	web.archive.org text/html Inactive Link Not Archived	 SUSE SUSE-SA:2006:028
No Description Provided	www.osvdb.org Inactive Link Not Archived	 OSVDB 24715
404: File not found	kernel.org text/plain Inactive Link Not Archived	 CONFIRM kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.16.8
Webmail - OVH	Vendor Advisory www.vupen.com text/html	 VUPEN ADV-2006-1399
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:10146
ASA-2006-161 (RHSA-2006-0493)	support.avaya.com text/html	 CONFIRM support.avaya.com/elmodocs2/security/ASA-2006-161.htm

Linux Kernel Multiple Vulnerabilities - Advisories - Secunia	web.archive.org text/html	 SECUNIA 21476
Advisories - Mandriva Linux	www.mandriva.com text/html	 MANDRIVA MDKSA-2006:086
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF linux-ip-route-input-dos(25872)
SUSE update for kernel - Advisories - Secunia	Vendor Advisory web.archive.org text/html	 SECUNIA 20398
Linux Kernel IP_ROUTE_INPUT Local Denial of Service Vulnerability	Patch cve.report (archive) text/html	 BID 17593

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	2.6.1	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	2.6.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.10	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.10	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.10	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.11	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.11	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.11	rc3	All	All

Operating System	Linux	Linux Kernel	2.6.11	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.11	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.11	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.11.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.12	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.12	All	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc6	All	All
Operating System	Linux	Linux Kernel	2.6.12.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.2	All	All	All

Operating System	Linux	Linux Kernel	2.6.12.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.13	All	All	All
Operating System	Linux	Linux Kernel	2.6.13	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.13	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.13	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.13	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.13	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.13	rc6	All	All
Operating System	Linux	Linux Kernel	2.6.13	rc7	All	All
Operating System	Linux	Linux Kernel	2.6.13.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.13.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.13.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.13.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.13.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.14	All	All	All
Operating System	Linux	Linux Kernel	2.6.14	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.14	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.14	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.14	rc4	All	All

Operating System	Linux	Linux Kernel	2.6.14	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.14.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.14.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.14.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.14.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.14.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.14.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.14.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.15	All	All	All
Operating System	Linux	Linux Kernel	2.6.15	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.15	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.15	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.15	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.15	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.15	rc6	All	All
Operating System	Linux	Linux Kernel	2.6.15	rc7	All	All
Operating System	Linux	Linux Kernel	2.6.15.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.15.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.15.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.15.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.15.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.15.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.15.7	All	All	All

Operating System	Linux	Linux Kernel	2.6.16	All	All	All
Operating System	Linux	Linux Kernel	2.6.16	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.16	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.16	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.16	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.16	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.16	rc6	All	All
Operating System	Linux	Linux Kernel	2.6.16.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.7	All	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	2.6.9	All	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	2.6.0	All	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	2.6.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.10	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.10	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.10	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.11	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.11	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.11	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.11	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.11	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.11.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.12	All	All	All

Operating System	Linux	Linux Kernel	2.6.11.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.12	All	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc6	All	All
Operating System	Linux	Linux Kernel	2.6.12.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.13	All	All	All
Operating System	Linux	Linux Kernel	2.6.13	rc1	All	All

Operating System	Linux	Linux Kernel	2.6.13	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.13	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.13	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.13	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.13	rc6	All	All
Operating System	Linux	Linux Kernel	2.6.13	rc7	All	All
Operating System	Linux	Linux Kernel	2.6.13.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.13.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.13.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.13.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.13.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.14	All	All	All
Operating System	Linux	Linux Kernel	2.6.14	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.14	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.14	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.14	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.14	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.14.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.14.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.14.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.14.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.14.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.14.6	All	All	All

Operating System	Linux	Linux Kernel	2.6.14.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.15	All	All	All
Operating System	Linux	Linux Kernel	2.6.15	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.15	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.15	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.15	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.15	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.15	rc6	All	All
Operating System	Linux	Linux Kernel	2.6.15	rc7	All	All
Operating System	Linux	Linux Kernel	2.6.15.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.15.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.15.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.15.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.15.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.15.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.15.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.16	All	All	All
Operating System	Linux	Linux Kernel	2.6.16	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.16	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.16	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.16	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.16	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.16	rc6	All	All

Operating System	Linux	Linux Kernel	2.6.16.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.7	All	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	2.6.9	All	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
cpe:2.3:o:linux:linux_kernel:2.6.0:*****:						
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:2.6.10:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.10:rc1:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.10:rc2:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.10:rc3:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.11:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.11:rc1:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.11:rc2:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.11:rc3:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.11:rc4:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.11:rc5:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.11.1:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.11.10:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.11.11:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.11.12:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.11.2:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.11.3:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.11.4:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.11.5:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.11.6:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.11.7:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.11.8:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.11.9:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.12:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.12:rc1:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.12:rc2:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.12:rc3:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.12:rc4:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.12:rc5:~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.12:rc6:~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.12.1:~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.12.2:~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.12.3:~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.12.4:~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.12.5:~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.12.6:~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.13:~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.13:rc1:~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.13:rc2:~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.13:rc3:~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.13:rc4:~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.13:rc5:~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.13:rc6:~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.13:rc7:~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.13.1:~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.13.2:~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.13.3:~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.13.4:~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.13.5:~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.14:~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.14:rc1:~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.14:rc2:~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.14:rc3:~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.14:rc4:~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.14:rc5:~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.14.1:~::~~::~~::~~::~~:::

cpe:2.3:o:linux:linux_kernel:2.6.14.2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.14.3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.14.4:*****:
cpe:2.3:o:linux:linux_kernel:2.6.14.5:*****:
cpe:2.3:o:linux:linux_kernel:2.6.14.6:*****:
cpe:2.3:o:linux:linux_kernel:2.6.14.7:*****:
cpe:2.3:o:linux:linux_kernel:2.6.15:*****:
cpe:2.3:o:linux:linux_kernel:2.6.15:rc1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.15:rc2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.15:rc3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.15:rc4:*****:
cpe:2.3:o:linux:linux_kernel:2.6.15:rc5:*****:
cpe:2.3:o:linux:linux_kernel:2.6.15:rc6:*****:
cpe:2.3:o:linux:linux_kernel:2.6.15:rc7:*****:
cpe:2.3:o:linux:linux_kernel:2.6.15.1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.15.2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.15.3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.15.4:*****:
cpe:2.3:o:linux:linux_kernel:2.6.15.5:*****:
cpe:2.3:o:linux:linux_kernel:2.6.15.6:*****:
cpe:2.3:o:linux:linux_kernel:2.6.15.7:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16:rc1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16:rc2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16:rc3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16:rc4:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16:rc5:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16:rc6:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.1:*****:

cpe:2.3:o:linux:linux_kernel:2.6.16.2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.4:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.5:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.6:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.7:*****:
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:2.6.9:****:*:
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:2.6.0:****:*:
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:2.6.10:****:*:
cpe:2.3:o:linux:linux_kernel:2.6.10:rc1:****:*:
cpe:2.3:o:linux:linux_kernel:2.6.10:rc2:****:*:
cpe:2.3:o:linux:linux_kernel:2.6.10:rc3:****:*:
cpe:2.3:o:linux:linux_kernel:2.6.11:****:*:
cpe:2.3:o:linux:linux_kernel:2.6.11:rc1:****:*:
cpe:2.3:o:linux:linux_kernel:2.6.11:rc2:****:*:
cpe:2.3:o:linux:linux_kernel:2.6.11:rc3:****:*:
cpe:2.3:o:linux:linux_kernel:2.6.11:rc4:****:*:
cpe:2.3:o:linux:linux_kernel:2.6.11:rc5:****:*:

cpe:2.3:o:linux:linux_kernel:2.6.11.rc5:*:*:*:*:*
cpe:2.3:o:linux:linux_kernel:2.6.11.1:*:*:*:*:*
cpe:2.3:o:linux:linux_kernel:2.6.11.10:*:*:*:*:*
cpe:2.3:o:linux:linux_kernel:2.6.11.11:*:*:*:*:*
cpe:2.3:o:linux:linux_kernel:2.6.11.12:*:*:*:*:*
cpe:2.3:o:linux:linux_kernel:2.6.11.2:*:*:*:*:*
cpe:2.3:o:linux:linux_kernel:2.6.11.3:*:*:*:*:*
cpe:2.3:o:linux:linux_kernel:2.6.11.4:*:*:*:*:*
cpe:2.3:o:linux:linux_kernel:2.6.11.5:*:*:*:*:*
cpe:2.3:o:linux:linux_kernel:2.6.11.6:*:*:*:*:*
cpe:2.3:o:linux:linux_kernel:2.6.11.7:*:*:*:*:*
cpe:2.3:o:linux:linux_kernel:2.6.11.8:*:*:*:*:*
cpe:2.3:o:linux:linux_kernel:2.6.11.9:*:*:*:*:*
cpe:2.3:o:linux:linux_kernel:2.6.12:*:*:*:*:*
cpe:2.3:o:linux:linux_kernel:2.6.12:rc1:*:*:*:*:*
cpe:2.3:o:linux:linux_kernel:2.6.12:rc2:*:*:*:*:*
cpe:2.3:o:linux:linux_kernel:2.6.12:rc3:*:*:*:*:*
cpe:2.3:o:linux:linux_kernel:2.6.12:rc4:*:*:*:*:*
cpe:2.3:o:linux:linux_kernel:2.6.12:rc5:*:*:*:*:*
cpe:2.3:o:linux:linux_kernel:2.6.12:rc6:*:*:*:*:*
cpe:2.3:o:linux:linux_kernel:2.6.12.1:*:*:*:*:*
cpe:2.3:o:linux:linux_kernel:2.6.12.2:*:*:*:*:*
cpe:2.3:o:linux:linux_kernel:2.6.12.3:*:*:*:*:*
cpe:2.3:o:linux:linux_kernel:2.6.12.4:*:*:*:*:*
cpe:2.3:o:linux:linux_kernel:2.6.12.5:*:*:*:*:*
cpe:2.3:o:linux:linux_kernel:2.6.12.6:*:*:*:*:*
cpe:2.3:o:linux:linux_kernel:2.6.13:*:*:*:*:*
cpe:2.3:o:linux:linux_kernel:2.6.13:rc1:*:*:*:*:*
cpe:2.3:o:linux:linux_kernel:2.6.13:rc2:*:*:*:*:*

cpe:2.3:o:linux:linux_kernel:2.6.13:rc3:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.13:rc4:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.13:rc5:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.13:rc6:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.13:rc7:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.13.1:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.13.2:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.13.3:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.13.4:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.13.5:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.14:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.14:rc1:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.14:rc2:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.14:rc3:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.14:rc4:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.14:rc5:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.14.1:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.14.2:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.14.3:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.14.4:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.14.5:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.14.6:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.14.7:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.15:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.15:rc1:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.15:rc2:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.15:rc3:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.15:rc4:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.15:rc5:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.15:rc6:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.15:rc7:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.15.1:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.15.2:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.15.3:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.15.4:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.15.5:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.15.6:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.15.7:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.16:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.16:rc1:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.16:rc2:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.16:rc3:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.16:rc4:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.16:rc5:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.16:rc6:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.16.1:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.16.2:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.16.3:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.16.4:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.16.5:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.16.6:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.16.7:*:*:*:*:*:
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:2.6.9:~::~~::~~::~~::~~::~~:::
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:~::~~::~~::~~::~~::~~::

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#)