

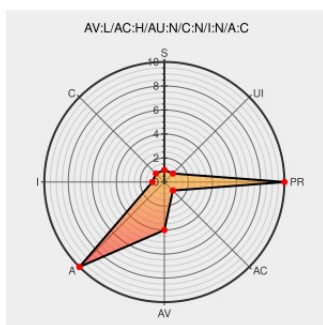


CVE-2006-6054

Published on: 11/21/2006 12:00:00 AM UTC

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

CVE-2006-6054

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

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

The ext2 file system code in Linux kernel 2.6.x allows local users to cause a denial of service (crash) via an ext2 stream with malformed data structures that triggers an error in the ext2_check_page due to a length that is smaller than the minimum.

CVE-2006-6054 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4 - MEDIUM**

Access
Vector

LOCAL

Access
Complexity

HIGH

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

Red Hat update for kernel - Advisories - Secunia

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

[X](#) [SECUNIA 26379](#)

Avaya Products Linux Kernel Multiple Vulnerabilities - Advisories - Secunia

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

[X](#) [SECUNIA 27528](#)

ASA-2007-404 (RHSA-2007-0672)

[support.avaya.com](#)
[text/html](#)

[G](#) [CONFIRM](#)
[support.avaya.com/elmodocs2/security/ASA-2007-404.htm](#)

Fedora Core Ext2 File System Denial of Service Vulnerability - Secunia Advisories - Vulnerability Intelligence - Secunia.com

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

[X](#) [SECUNIA 22837](#)

usn/usn-416-1 - Ubuntu: Linux for human beings

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

[U](#) [UBUNTU USN-416-1](#)

rhnl.redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2007:0673
Month of Kernel Bugs (MoKB): Linux 2.6.x ext2_check_page denial of service	Exploit Vendor Advisory web.archive.org text/html Inactive Link Not Archived	 MISC projects.info-pull.com/mokb/MOKB-12-11-2006.html
Security Announcement	web.archive.org text/html Inactive Link Not Archived	 SUSE SUSE-SA:2006:079
Ubuntu update for kernel - Advisories - Secunia	Vendor Advisory web.archive.org text/html	 SECUNIA 24098
rhnl.redhat.com Red Hat Support	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2007:0014
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF kernel-ext2-filesystem-dos(30201)
Debian -- Security Information -- DSA-1504-1 kernel-source-2.6.8	www.debian.org Deprecated Link text/html	 DEBIAN DSA-1504
SUSE update for kernel - Advisories - Secunia	web.archive.org text/html	 SECUNIA 23474
Red Hat update for kernel - Advisories - Secunia	Vendor Advisory web.archive.org text/html	 SECUNIA 23997
rPath update for kernel and xen - Advisories - Secunia	web.archive.org text/html	 SECUNIA 25691
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:10006
Webmail - OVH	www.vupen.com text/html	 VUPEN ADV-2006-4487
Avaya Products Kernel Multiple Vulnerabilities - Advisories - Secunia	Vendor Advisory web.archive.org text/html	 SECUNIA 24206
rhnl.redhat.com Red Hat Support	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2007:0436
Debian -- Security Information -- DSA-1503-1 kernel-source-2.4.27	www.debian.org Deprecated Link text/html	 DEBIAN DSA-1503
Red Hat update for kernel - Advisories - Secunia	web.archive.org text/html	 SECUNIA 25630
SecurityFocus	www.securityfocus.com text/html	 BUGTRAQ 20070615 rPSA-2007-0124-1 kernel xen
rhnl.redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2007:0672
Debian update for kernel - Secunia Advisories - Vulnerability Information - Secunia.com	web.archive.org text/html	 SECUNIA 29058

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	2.6.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.11	All	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

System						
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	2.6.13.1	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	2.6.14.1	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	2.6.15.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.15.2	All	All	All

System						
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	2.6.16.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.12	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.13	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.14	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.15	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.16	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.17	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.18	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.19	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.20	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.21	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.22	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.23	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.24	All	All	All

System						
Operating System	Linux	Linux Kernel	2.6.16.25	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.26	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.27	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.28	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.29	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.30	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.31	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.32	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.33	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	2.6.16.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.17	All	All	All
Operating System	Linux	Linux Kernel	2.6.17.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.17.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.17.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.17.12	All	All	All
Operating System	Linux	Linux Kernel	2.6.17.13	All	All	All
Operating System	Linux	Linux Kernel	2.6.17.14	All	All	All

System						
Operating System	Linux	Linux Kernel	2.6.17.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.17.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.17.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.17.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.17.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.17.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.17.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.17.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.18	All	All	All
Operating System	Linux	Linux Kernel	2.6.18.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.18.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.18.3	All	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	2.6.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.8.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.9	2.6.20	All	All
Operating System	Linux	Linux Kernel	2.6.0	All	All	All
Operating	Linux	Linux Kernel	2.6.1	All	All	All

System						
Operating System	Linux	Linux Kernel	2.6.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.11	All	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	2.6.12.1	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	Linux	Linux Kernel	2.6.13.1	All	All	All

System						
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	2.6.14.1	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	2.6.15.1	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	2.6.16.1	All	All	All
Operating	Linux	Linux Kernel	2.6.16.10	All	All	All

System						
Operating System	Linux	Linux Kernel	2.6.16.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.12	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.13	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.14	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.15	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.16	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.17	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.18	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.19	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.20	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.21	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.22	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.23	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.24	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.25	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.26	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.27	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.28	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.29	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.30	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.31	All	All	All

Operating System	Linux	Linux Kernel	2.6.16.32	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.32	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.33	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	2.6.16.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.17	All	All	All
Operating System	Linux	Linux Kernel	2.6.17.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.17.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.17.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.17.12	All	All	All
Operating System	Linux	Linux Kernel	2.6.17.13	All	All	All
Operating System	Linux	Linux Kernel	2.6.17.14	All	All	All
Operating System	Linux	Linux Kernel	2.6.17.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.17.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.17.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.17.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.17.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.17.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.17.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.17.9	All	All	All

Operating System	Linux	Linux Kernel	2.6.17.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.18	All	All	All
Operating System	Linux	Linux Kernel	2.6.18.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.18.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.18.3	All	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	2.6.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.8.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.9	2.6.20	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:2.6.10:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.11:*:*:*:*:*:						
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:2.6.11.5:*****:
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:2.6.12.1:*****:
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:2.6.13.1:*****:
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:2.6.14.1:*****:
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:2.6.15.1:*****:
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:2.6.16.1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.10:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.11:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.12:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.13:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.14:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.15:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.16:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.17:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.18:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.19:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.20:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.21:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.22:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.23:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.24:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.25:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.26:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.27:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.28:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.29:*****:

cpe:2.3:o:linux:linux_kernel:2.6.16.3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.30:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.31:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.32:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.33:*****:
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:2.6.16.8:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.9:*****:
cpe:2.3:o:linux:linux_kernel:2.6.17:*****:
cpe:2.3:o:linux:linux_kernel:2.6.17.1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.17.10:*****:
cpe:2.3:o:linux:linux_kernel:2.6.17.11:*****:
cpe:2.3:o:linux:linux_kernel:2.6.17.12:*****:
cpe:2.3:o:linux:linux_kernel:2.6.17.13:*****:
cpe:2.3:o:linux:linux_kernel:2.6.17.14:*****:
cpe:2.3:o:linux:linux_kernel:2.6.17.2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.17.3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.17.4:*****:
cpe:2.3:o:linux:linux_kernel:2.6.17.5:*****:
cpe:2.3:o:linux:linux_kernel:2.6.17.6:*****:
cpe:2.3:o:linux:linux_kernel:2.6.17.7:*****:
cpe:2.3:o:linux:linux_kernel:2.6.17.8:*****:
cpe:2.3:o:linux:linux_kernel:2.6.17.9:*****:
cpe:2.3:o:linux:linux_kernel:2.6.18:*****:
cpe:2.3:o:linux:linux_kernel:2.6.18.1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.18.2:*****:

cpe:2.3:o:linux:linux_kernel:2.6.18.3:~::~~::~~::~~::~~::~~::~~:::
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:2.6.7:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.8:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.8.1:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.9:2.6.20:~::~~::~~::~~::~~::~~::~~:::
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:2.6.10:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.11:~::~~::~~::~~::~~::~~::~~:::
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:2.6.12.1:~::~~::~~::~~::~~::~~::~~:::

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:2.6.13.1:*****:
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:2.6.14.1:*****:
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:2.6.15.1:*****:
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:2.6.16.1:*****:

cpe:2.3:o:linux:linux_kernel:2.6.16.10:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.11:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.12:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.13:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.14:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.15:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.16:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.17:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.18:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.19:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.20:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.21:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.22:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.23:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.24:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.25:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.26:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.27:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.28:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.29:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.30:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.31:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.32:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.33:*****:
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:2.6.16.8:*****:
cpe:2.3:o:linux:linux_kernel:2.6.16.9:*****:
cpe:2.3:o:linux:linux_kernel:2.6.17:*****:
cpe:2.3:o:linux:linux_kernel:2.6.17.1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.17.10:*****:
cpe:2.3:o:linux:linux_kernel:2.6.17.11:*****:
cpe:2.3:o:linux:linux_kernel:2.6.17.12:*****:
cpe:2.3:o:linux:linux_kernel:2.6.17.13:*****:
cpe:2.3:o:linux:linux_kernel:2.6.17.14:*****:
cpe:2.3:o:linux:linux_kernel:2.6.17.2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.17.3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.17.4:*****:
cpe:2.3:o:linux:linux_kernel:2.6.17.5:*****:
cpe:2.3:o:linux:linux_kernel:2.6.17.6:*****:
cpe:2.3:o:linux:linux_kernel:2.6.17.7:*****:
cpe:2.3:o:linux:linux_kernel:2.6.17.8:*****:
cpe:2.3:o:linux:linux_kernel:2.6.17.9:*****:
cpe:2.3:o:linux:linux_kernel:2.6.18:*****:
cpe:2.3:o:linux:linux_kernel:2.6.18.1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.18.2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.18.3:*****:
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:2.6.7:*****:

```
cpe:2.3.0:linux:linux_kernel:2.6.7 : : : : : :
```

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

```
cpe:2.3:o:linux:linux_kernel:2.6.8.1:*:*:*:*:*:
```

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

[← 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