



CVE-2009-2847

Published on: 08/18/2009 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:30 PM UTC

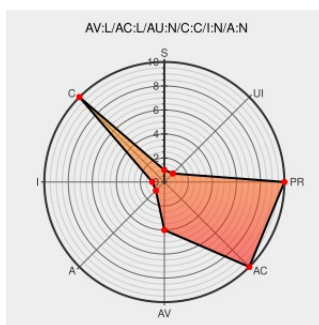
CVE-2009-2847

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

The `do_sigaltstack` function in `kernel/signal.c` in Linux kernel 2.4 through 2.4.37 and 2.6 before 2.6.31-rc5, when running on 64-bit systems, does not clear certain padding bytes from a structure, which allows local users to obtain sensitive information from the kernel stack via the `sigaltstack` function.

CVE-2009-2847 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

COMPLETE

Integrity
Impact

NONE

Availability
Impact

NONE

CVE References

Description

Tags

Link

Support

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

[REDHAT RHSA-2009:1438](#)

Linux Kernel "sigaltstack()" Information Disclosure - Secunia Advisories - Vulnerability Information - Secunia.com

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

[SECUNIA 36136](#)

oss-security - CVE request - kernel: information leak in sigaltstack

[Patch](#)
www.openwall.com
[text/html](#)

[MLIST \[oss-security\] 20090804 CVE request - kernel: information leak in sigaltstack](#)

Repository / Oval Repository

oval.cisecurity.org
[text/html](#)

[OVAL oval:org.mitre.oval:def:8405](#)

Hed Hat update for kernel - Secunia Advisories - Vulnerability Information - Secunia.com	web.archive.org text/html	 SECUNIA 36759
SecurityFocus	www.securityfocus.com text/html	 BUGTRAQ 20091120 VMSA-2009-0016 VMware vCenter and ESX update release and vMA patch release address multiple security issue in third party components
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:10637
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	 VUPEN ADV-2009-3316
Ubuntu update for kernel - Secunia Advisories - Vulnerability Information - Secunia.com	web.archive.org text/html	 SECUNIA 37105
Linux Kernel <= 2.6.31-rc5 sigaltstack 4-Byte Stack Disclosure Exploit	www.exploit-db.com Proof of Concept text/x-c	 EXPLOIT-DB 9352
[SECURITY] Fedora 11 Update: kernel-2.6.29.6-217.2.16.fc11	www.redhat.com text/html	 FEDORA FEDORA-2009-9044
kernel/git/torvalds/linux.git - Linux kernel source tree	Exploit git.kernel.org text/html	 CONFIRM git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commitdiff;h=0083fc2c50e6c5127c2802ad323adf8143ab7856
Red Hat update for kernel - Secunia.com	web.archive.org text/html	 SECUNIA 36562
oss-security - Re: CVE request - kernel: information leak in sigaltstack	Patch www.openwall.com text/html	 MLIST [oss-security] 20090805 Re: CVE request - kernel: information leak in sigaltstack
oss-security - Re: CVE request - kernel: information leak in sigaltstack	www.openwall.com text/html	 MLIST [oss-security] 20090826 Re: CVE request - kernel: information leak in sigaltstack
USN-852-1: Linux kernel vulnerabilities Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-852-1
VMSA-2009-0016.1	www.vmware.com text/html	 CONFIRM www.vmware.com/security/advisories/VMSA-2009-0016.html
rhn.redhat.com Red Hat Support	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2009:1243
Fedora update for kernel - Secunia Advisories - Vulnerability Information - Secunia.com	web.archive.org text/html	 SECUNIA 36501
Bug 515392 – CVE-2009-2847 kernel: information leak in sigaltstack	Patch bugzilla.redhat.com text/html	 CONFIRM bugzilla.redhat.com/show_bug.cgi?id=515392
VMware ESX and vMA Update for Multiple Packages - Secunia Advisories - Vulnerability Information - Secunia.com	web.archive.org text/html	 SECUNIA 37471

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
Application	Linux	Kernel	2.6.24.7	All	All	All
Application	Linux	Kernel	2.6.25.15	All	All	All
Application	Linux	Kernel	2.6.24.7	All	All	All
Application	Linux	Kernel	2.6.25.15	All	All	All
Hardware 	Linux	Linux	All	All	x64	All
Hardware 	Linux	Linux	All	All	x64	All
Operating System	Linux	Linux Kernel	2.6	All	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	2.6.10	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 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
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
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	2.6.16.31	-rc1	All	All
Operating System	Linux	Linux Kernel	2.6.16.31	-rc2	All	All
Operating System	Linux	Linux Kernel	2.6.16.31	-rc3	All	All
Operating System	Linux	Linux Kernel	2.6.16.31	-rc4	All	All
Operating System	Linux	Linux Kernel	2.6	All	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	2.6.10	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 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
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
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	2.6.16.31	-rc1	All	All
Operating System	Linux	Linux Kernel	2.6.16.31	-rc2	All	All
Operating System	Linux	Linux Kernel	2.6.16.31	-rc3	All	All
Operating System	Linux	Linux Kernel	2.6.16.31	-rc4	All	All
Operating System	Linux	Linux Kernel	All	-rc5	All	All
cpe:2.3:a:linux:kernel:2.6.24.7:*:*:*:*:*::						

cpe:2.3:a:linux:kernel:2.6.25.15:*:*:*:*:*:
cpe:2.3:a:linux:kernel:2.6.24.7:*:*:*:*:*:
cpe:2.3:a:linux:kernel:2.6.25.15:*:*:*:*:*:
cpe:2.3:h:linux:linux:*:*:x64:*:*:*:*:
cpe:2.3:h:linux:linux:*:*:x64:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6:*:*:*:*:*:
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:2.3:0: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:2.6.16.31:-rc1:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.16.31:-rc2:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.16.31:-rc3:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.16.31:-rc4:*:*:*:*:*:
```

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

```
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:2.6.16.31:-rc1:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.16.31:-rc2:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.16.31:-rc3:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.16.31:-rc4:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:*:-rc5:*:*:*:*:*: