

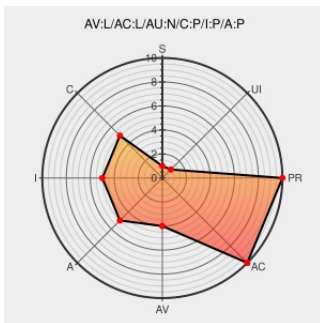


CVE-2005-2555

Published on: 08/16/2005 12:00:00 AM UTC

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

CVE-2005-2555

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

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

Linux kernel 2.6.x does not properly restrict socket policy access to users with the CAP_NET_ADMIN capability, which could allow local users to conduct unauthorized activities via (1) ipv4/ip_sockglue.c and (2) ipv6/ipv6_sockglue.c.

CVE-2005-2555 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.6 - MEDIUM**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

rhnl.redhat.com | Red Hat Support

Not Applicable
[www.redhat.com](#)
text/html

[REDHAT RHSA-2005:663](#)

Secunia - Advisories - Debian update
for kernel-source-2.4.27

Permissions Required
Third Party Advisory
[web.archive.org](#)
text/html

[SECUNIA 19369](#)

Security Announcement

Broken Link
[web.archive.org](#)
text/html
Inactive Link Not Archived

[SUSE SUSE-SA:2005:050](#)

Webmail - OVH

Broken Link
[www.vupen.com](#)
text/html

[VUPEN ADV-2005-1878](#)

kernel/git/torvalds/linux.git - Linux kernel source tree	text/html Issue Tracking www.kernel.org text/html	 CONFIRM www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=6fc0b4a7a73a81e74d0004732df358f4f9975be2
Advisories - Mandriva Linux	www.mandriva.com text/html	 MANDRAKE MDKSA-2005:219
Advisories - Mandriva Linux	Broken Link www.mandriva.com text/html	 MANDRAKE MDKSA-2005:218
Debian update for kernel-source-2.6.8 - Advisories - Secunia	Permissions Required Third Party Advisory web.archive.org text/html	 SECUNIA 19374
SecurityFocus	www.securityfocus.com text/html	 FEDORA FLSA:157459-3
rhn.redhat.com Red Hat Support	Not Applicable www.redhat.com text/html	 REDHAT RHSA-2005:514
Debian -- Security Information -- DSA-1018-2 kernel-source-2.4.27	Third Party Advisory www.debian.org Deprecated Link text/html	 DEBIAN DSA-1018
Secunia - Advisories - Red Hat update for kernel	Permissions Required Third Party Advisory web.archive.org text/html	 SECUNIA 17002
Secunia - Advisories - Red Hat update for kernel	Permissions Required Third Party Advisory web.archive.org text/html	 SECUNIA 17073
USN-169-1: Linux kernel vulnerabilities Ubuntu security notices	usn.ubuntu.com text/html	 UBUNTU USN-169-1
kernel/git/torvalds/linux.git - Linux kernel source tree	Issue Tracking www.kernel.org text/html	 CONFIRM www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commitdiff;h=6fc0b4a7a73a81e74d0004732df358f4f9975be2
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:10444
Debian -- Security Information -- DSA-1017-1 kernel-source-2.6.8	www.debian.org Deprecated Link text/html	 DEBIAN DSA-1017
Secunia - Advisories - Mandriva update for kernel	Permissions Required Third Party Advisory web.archive.org text/html	 SECUNIA 17826
Linux Kernel IPSec Policies Authorization Bypass Vulnerability	Third Party Advisory VDB Entry cve.report (archive) text/html	 BID 14609

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,

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	3.1	All	All	All
Operating System	Debian	Debian Linux	3.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.0	All	All	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	2.6.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.10	rc2	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	2.6.11.1	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_rc1_bk6	All	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc4	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	2.6.6	rc1	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	2.6.8	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	2.6.8.1	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	2.6.20	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	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	2.6.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.10	rc2	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	2.6.11.1	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_rc1_bk6	All	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc4	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	2.6.6	rc1	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	2.6.8	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	2.6.8.1	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	2.6.20	All	All
Operating System	Linux	Linux Kernel	2.6_test9_cvs	All	All	All
cpe:2.3:o:debian:debian_linux:3.1:****:*:*:						
cpe:2.3:o:debian:debian_linux:3.1:****:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.0:*****:*:						
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:2.6.10:*:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.10:rc2:*:*:*:*:*:
```

```
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:2.6.11.1:::*:*:*:*:*:
```

```
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_rc1_bk6:*:*:*:*:*:
```

cpe:2.3:o:linux:linux_kernel:2.6.12:rc1:~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.12:rc4:~::~~::~~::~~::~~::~~:::
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:2.6.6:rc1:~::~~::~~::~~::~~::~~:::
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:2.6.8:~::~~::~~::~~::~~::~~:::
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:2.6.8.1:~::~~::~~::~~::~~::~~:::
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:2.6.9:2.6.20:*:*:*:*:
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: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:2.6.10:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.10:rc2:*:*:*:*:*:
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:2.6.11.1:*:*:*:*:*:
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_rc1_bk6:****:*:
cpe:2.3:o:linux:linux_kernel:2.6.12:rc1:****:*:
cpe:2.3:o:linux:linux_kernel:2.6.12:rc4:****:*:
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:2.6.6:rc1:****:*:
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:2.6.8:****:*:
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:2.6.8.1:****:*:
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:2.6.9:2.6.20:****:
cpe:2.3:o:linux:linux_kernel:2.6_test9_cvs:****:

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](#)