



CVE-2006-1864

Published on: 04/26/2006 12:00:00 AM UTC

Last Modified on: 02/13/2023 02:10:36 AM UTC

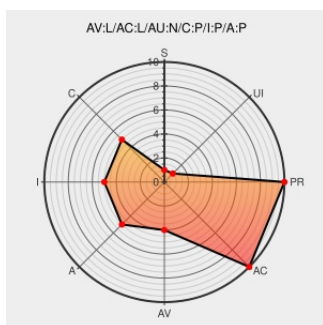
CVE-2006-1864

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

Directory traversal vulnerability in smbfs in Linux 2.6.16 and earlier allows local users to escape chroot restrictions for an SMB-mounted filesystem via "..\" sequences, a similar vulnerability to CVE-2006-1863.

CVE-2006-1864 has been assigned by secalert@redhat.com 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

Advisories - Mandriva Linux

[www.mandriva.com](http://www.mandriva.com/text/html)
text/html

[MANDRIVA MDKSA-2006:151](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](https://exchange.xforce.ibmcloud.com/text/html)
text/html

[XF kernel-smbfs-directory-traversal\(26137\)](#)

Advisories - Mandriva Linux

[www.mandriva.com](http://www.mandriva.com/text/html)
text/html

[MANDRIVA MDKSA-2006:150](#)

Repository / Oval Repository

[oval.cisecurity.org](https://oval.cisecurity.org/text/html)
text/html

[OVAL oval:org.mitre.oval:def:11327](#)

SecurityFocus

[www.securityfocus.com](http://www.securityfocus.com/text/html)
text/html

[BUGTRAQ 20061113 VMSA-2006-0007 - VMware ESX Server 2.1.3 Upgrade Patch 2](#)

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

[web.archive.org](http://web.archive.org/text/html)
text/html

[SECUNIA 20914](#)

Webmail - OVH	www.vupen.com text/html	VUPEN ADV-2006-2554
Ubuntu update for kernel - Advisories - Secunia	web.archive.org text/html	SECUNIA 20716
VMware ESX Server 2.0.2 Upgrade Patch 2 (for 2.0.2 Systems)	www.vmware.com text/html	CONFIRM www.vmware.com/download/esx/esx-202-200610-patch.html
Red Hat update for kernel - Advisories - Secunia	web.archive.org text/html	SECUNIA 21035
Avaya Products Linux Kernel Multiple Vulnerabilities - Advisories - Secunia	web.archive.org text/html	SECUNIA 23064
Red Hat update for kernel - Advisories - Secunia	web.archive.org text/html	SECUNIA 20237
Avaya Products Linux Kernel Multiple Vulnerabilities - Advisories - Secunia	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
VMware ESX Server Multiple Vulnerabilities - Advisories - Secunia	web.archive.org text/html	SECUNIA 22875
VMware ESX Server 2.1.3 Upgrade Patch 2 (for 2.1.3 Systems Only)	www.vmware.com text/html	CONFIRM www.vmware.com/download/esx/esx-213-200610-patch.html
VMware ESX Server 2.5.4 Upgrade Patch 1 (for 2.5.4 Systems Only)	www.vmware.com text/html	CONFIRM www.vmware.com/download/esx/esx-254-200610-patch.html
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 25067
ASA-2006-254 (RHSA-2006-0710)	support.avaya.com text/html	CONFIRM support.avaya.com/elmodocs2/security/ASA-2006-254.htm
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20061113 VMsa-2006-0008 - VMware ESX Server 2.0.2 Upgrade Patch 2
Linux Kernel SMBFS CHRoot Security Restriction Bypass Vulnerability	cve.report (archive) text/html	BID 17735
Debian update for kernel-source-2.4.27 - Advisories - Secunia	web.archive.org text/html	SECUNIA 20671
Red Hat update for kernel - Advisories - Secunia	web.archive.org text/html	SECUNIA 22497
Mandriva update for kernel - Secunia Advisories - Vulnerability Information - Secunia.com	web.archive.org text/html	SECUNIA 21614
Linux Kernel SMBFS chroot Directory Traversal Vulnerability - Advisories - Secunia	web.archive.org text/html	SECUNIA 19869
rh.n.redhat.com Red Hat Support	www.redhat.com text/html	REDHAT RHSA-2006:0493
usn/usn-302-1 - Ubuntu: Linux for human beings	www.ubuntu.com text/html	UBUNTU USN-302-1

text/html

SecurityFocus

www.securityfocus.com

text/html

 BUGTRAQ 20061113 VMSA-2006-0006 - VMware ESX Server 2.5.3 Upgrade Patch 4

rhnl.redhat.com | Red Hat Support

www.redhat.com

text/html

 REDHAT RHSA-2006:0710

Debian -- Security Information -- DSA-1103-1 kernel-source-2.6.8

www.debian.org

Depreciated Link

text/html

 DEBIAN DSA-1103

Security Announcement

web.archive.org

text/html

Inactive Link Not Archived

 SUSE SUSE-SA:2006:028

Webmail - OVH

www.vupen.com

text/html

 VUPEN ADV-2006-4502

SecurityFocus

www.securityfocus.com

text/html

 BUGTRAQ 20061113 VMSA-2006-0005 - VMware ESX Server 2.5.4 Upgrade Patch 1

rhnl.redhat.com | Red Hat Support

www.redhat.com

text/html

 REDHAT RHSA-2006:0579

rhnl.redhat.com | Red Hat Support

www.redhat.com

text/html

 REDHAT RHSA-2006:0580

189435 – CVE-2006-1864 smbfs chroot issue

Exploit

bugzilla.redhat.com

text/html

 CONFIRM
bugzilla.redhat.com/bugzilla/show_bug.cgi?id=189435

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

www.trustix.org

text/plain

Inactive Link Not Archived

 TRUSTIX 2006-0026

SUSE update for kernel - Advisories - Secunia

web.archive.org

text/html

 SECUNIA 20398

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	2.6.16	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	2.6.16.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.16_rc7	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	2.6.16.7	All	All	All

$\sim j \sim \dots$

Operating System	Linux	Linux Kernel	2.6.16.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.16_rc7	All	All	All
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:2.6.16.7:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.16.8:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.16_rc7:*:*:*:*:*:						
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:2.6.16.7:*:*:*:*:*:						

```
cpe:2.3:o:linux:linux_kernel:2.6.16_rc7:*:*:*:*:*:*:
```

[← Previous ID](#)

Next ID→

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.report and Source URL Uptime Status status.cve.report