



CVE-2006-1343

Published on: 03/21/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:01 PM UTC

CVE-2006-1343

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

net/ipv4/netfilter/ip_conntrack_core.c in Linux kernel 2.4 and 2.6, and possibly net/ipv4/netfilter/nf_conntrack_l3proto_ipv4.c in 2.6, does not clear sockaddr_in.sin_zero before returning IPv4 socket names from the getsockopt function with SO_ORIGINAL_DST, which allows local users to obtain portions of potentially sensitive memory.

CVE-2006-1343 has been assigned by [security-info@sgi.com](#) to track the vulnerability

CVSS2 Score: **2.1 - LOW**

Access Vector

LOCAL

Access Complexity

LOW

Authentication

NONE

Confidentiality Impact

PARTIAL

Integrity Impact

NONE

Availability Impact

NONE

CVE References

Description

Tags

Link

Advisories - Mandriva Linux

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

[MANDRIVA MDKSA-2006:150](#)

No Description Provided

[www.osvdb.org](#)

[OSVDB 29841](#)

Inactive Link **Not Archived**

ASA-2006-200 (RHSA-2006-0575)

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

[CONFIRM](#)
[support.avaya.com/elmodocs2/security/ASA-2006-200.htm](#)

SecurityFocus

[www.securityfocus.com](#)
[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 -

[web.archive.org](#)

[SECUNIA 22093](#)

Secunia	text/html	
Red Hat update for kernel - Advisories - Secunia	web.archive.org text/html	 SECUNIA 21136
Advisories - Mandriva Linux	www.mandriva.com text/html	 MANDRIVA MDKSA-2006:123
ASA-2006-180 (RHSA-2006-0437)	support.avaya.com text/html	 CONFIRM support.avaya.com/elmodocs2/security/ASA-2006-180.htm
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
rhn.redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2006:0437
'BUG: Small information leak in SO_ORIGINAL_DST (2.4 and 2.6) and' - MARC	marc.info text/x-c	 MLIST [linux-netdev] 20060304 BUG: Small information leak in SO_ORIGINAL_DST (2.4 and 2.6) and
Debian -- Security Information -- DSA-1097-1 kernel-source-2.4.27	www.debian.org text/html Deprecated Link	 DEBIAN DSA-1097
	www.trustix.org text/plain Inactive Link Not Archived	 TRUSTIX 2006-0032
VMware ESX Server Multiple Vulnerabilities - Advisories - Secunia	web.archive.org text/html	 SECUNIA 22875
USN-281-1: Linux kernel vulnerabilities Ubuntu security notices	usn.ubuntu.com text/html	 UBUNTU USN-281-1
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
Linux Kernel Ssockaddr_In.Sin_Zero Kernel Memory Disclosure Vulnerabilities	cve.report (archive) text/html	 BID 17203
Secunia - Advisories - Ubuntu update for kernel	web.archive.org text/html	 SECUNIA 19955
Mandriva update for kernel - Advisories - Secunia	web.archive.org text/html	 SECUNIA 21045
SecurityFocus	www.securityfocus.com text/html	 BUGTRAQ 20061113 VMSA-2006-0008 - VMware ESX Server 2.0.2 Upgrade Patch 2
Debian update for kernel-source-2.4.27 - Advisories - Secunia	web.archive.org text/html	 SECUNIA 20671
rhn.redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2006:0575
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:10875
SecurityFocus	www.securityfocus.com text/html	 BUGTRAQ 20061113 VMSA-2006-0006 - VMware ESX Server 2.5.3 Upgrade Patch 4
Webmail - OVH	www.vupen.com text/html	 VUPEN ADV-2006-2071

Linux Kernel IPv4 "sockaddr_in.sin_zero" Information Disclosure - Advisories - Secunia	web.archive.org text/html	 SECUNIA 19357
Webmail - OVH	www.vupen.com text/html	 VUPEN ADV-2006-4502
Debian -- Security Information -- DSA-1184-2 kernel-source-2.6.8	www.debian.org text/html Deprecated Link	 DEBIAN DSA-1184
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
Red Hat update for kernel - Advisories - Secunia	web.archive.org text/html	 SECUNIA 21465
Avaya Products Linux Kernel Multiple Vulnerabilities - Advisories - Secunia	web.archive.org text/html	 SECUNIA 21983
Avaya Products Linux Kernel Multiple Vulnerabilities - Advisories - Secunia	web.archive.org text/html	 SECUNIA 22417
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF linux-sockaddr-memory-leak(25425)
SecurityFocus	www.securityfocus.com text/html	 BUGTRAQ 20060531 rPSA-2006-0087-1 kernel

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	2.4.0	All	All	All
Operating System	Linux	Linux Kernel	2.6.0	All	All	All
Operating System	Linux	Linux Kernel	2.4.0	All	All	All
Operating System	Linux	Linux Kernel	2.6.0	All	All	All
cpe:2.3:o:linux:linux_kernel:2.4.0:*:*:*:*:*.*						
cpe:2.3:o:linux:linux_kernel:2.6.0:*:*:*:*:*.*						
cpe:2.3:o:linux:linux_kernel:2.4.0:*:*:*:*:*.*						

```
cpe:2.3:o:linux:linux_kernel:2.6.0.*.*.*.*.*.*.*.*.*.*
```

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