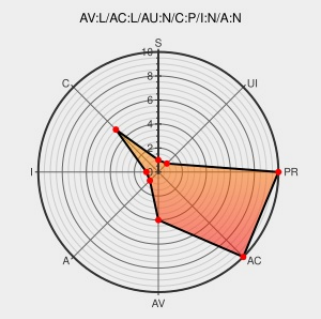
# CVE-2006-1343

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 | Access Complexity | Authentication |
|---|---|---|
| LOCAL | LOW | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| PARTIAL | NONE | NONE |

### CVE References

| Description | Tags | Link |
|---|---|---|
| Advisories - Mandriva Linux | www.mandriva.com text/html | MANDRIVA MDKSA-2006:150 |
| No Description Provided | www.osvdb.org Inactive Link Not Archived | OSVDB 29841 |
| 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<br>text/html | SECUNIA 21136 |
| Advisories - Mandriva Linux | www.mandriva.com<br>text/html | MANDRIVA MDKSA-2006:123 |
| ASA-2006-180 (RHSA-2006-0437) | support.avaya.com<br>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<br>text/html | CONFIRM www.vmware.com/download/esx/esx-202-200610-patch.html |
| rhn.redhat.com \| Red Hat Support | www.redhat.com<br>text/html | REDHAT RHSA-2006:0437 |
| 'BUG: Small information leak in SO_ORIGINAL_DST (2.4 and 2.6) and' - MARC | marc.info<br>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<br>Depreciated Link<br>text/html | DEBIAN DSA-1097 |
| | www.trustix.org<br>text/plain<br>Inactive Link Not Archived | TRUSTIX 2006-0032 |
| VMware ESX Server Multiple Vulnerabilities - Advisories - Secunia | web.archive.org<br>text/html | SECUNIA 22875 |
| USN-281-1: Linux kernel vulnerabilities \| Ubuntu security notices | usn.ubuntu.com<br>text/html | UBUNTU USN-281-1 |
| VMware ESX Server 2.1.3 Upgrade Patch 2 (for 2.1.3 Systems Only) | www.vmware.com<br>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<br>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)<br>text/html | BID 17203 |
| Secunia - Advisories - Ubuntu update for kernel | web.archive.org<br>text/html | SECUNIA 19955 |
| Mandriva update for kernel - Advisories - Secunia | web.archive.org<br>text/html | SECUNIA 21045 |
| SecurityFocus | www.securityfocus.com<br>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<br>text/html | SECUNIA 20671 |
| rhn.redhat.com \| Red Hat Support | www.redhat.com<br>text/html | REDHAT RHSA-2006:0575 |
| Repository / Oval Repository | oval.cisecurity.org<br>text/html | OVAL oval:org.mitre.oval:def:10875 |
| SecurityFocus | www.securityfocus.com<br>text/html | BUGTRAQ 20061113 VMSA-2006-0006 - VMware ESX Server 2.5.3 Upgrade Patch 4 |
| Webmail - OVH | www.vupen.com<br>text/html | VUPEN ADV-2006-2071 |

| | | |
|---|---|---|
| Linux Kernel IPv4 "sockaddr_in.sin_zero" Information Disclosure - Advisories - Secunia | web.archive.org<br>text/html | SECUNIA 19357 |
| Webmail - OVH | www.vupen.com<br>text/html | VUPEN ADV-2006-4502 |
| Debian -- Security Information -- DSA-1184-2 kernel-source-2.6.8 | www.debian.org<br>Depreciated Link<br>text/html | DEBIAN DSA-1184 |
| SecurityFocus | www.securityfocus.com<br>text/html | BUGTRAQ 20061113 VMSA-2006-0005 - VMware ESX Server 2.5.4 Upgrade Patch 1 |
| rhn.redhat.com \| Red Hat Support | www.redhat.com<br>text/html | REDHAT RHSA-2006:0579 |
| rhn.redhat.com \| Red Hat Support | www.redhat.com<br>text/html | REDHAT RHSA-2006:0580 |
| Red Hat update for kernel - Advisories - Secunia | web.archive.org<br>text/html | SECUNIA 21465 |
| Avaya Products Linux Kernel Multiple Vulnerabilities - Advisories - Secunia | web.archive.org<br>text/html | SECUNIA 21983 |
| Avaya Products Linux Kernel Multiple Vulnerabilities - Advisories - Secunia | web.archive.org<br>text/html | SECUNIA 22417 |
| IBM X-Force Exchange | exchange.xforce.ibmcloud.com<br>text/html | XF linux-sockaddr-memory-leak(25425) |
| SecurityFocus | www.securityfocus.com<br>text/html | BUGTRAQ 20060531 rPSA-2006-0087-1 kernel |



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→