



CVE-2008-2812

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

| | |
|------------------------|--|
| CVE | CVE-2008-2812 |
| State | PUBLIC |
| Assigner | secalert@redhat.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2008-07-09 00:41:00 UTC |
| Updated | 2023-02-13 02:19:00 UTC |
| Description | The Linux kernel before 2.6.25.10 does not properly perform tty operations, which allows local users to cause a denial of se |

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|--------|-------------------------------|---------|--------|---------|----------|
| Application | Avaya | Communication Manager | All | All | All | All |
| Application | Avaya | Communication Manager | All | All | All | All |
| Application | Avaya | Expanded Meet-me Conferencing | All | All | All | All |
| Application | Avaya | Expanded Meet-me Conferencing | All | All | All | All |
| Application | Avaya | Intuity Audix Lx | 2.0 | All | All | All |
| Application | Avaya | Intuity Audix Lx | 2.0 | All | All | All |
| Application | Avaya | Meeting Exchange | 5.0 | All | All | All |
| Application | Avaya | Meeting Exchange | 5.0 | All | All | All |
| Application | Avaya | Message Networking | 3.1 | All | All | All |
| Application | Avaya | Message Networking | 3.1 | All | All | All |
| Application | Avaya | Messaging Storage Server | 4.0 | All | All | All |
| Application | Avaya | Messaging Storage Server | 4.0 | All | All | All |
| Application | Avaya | Proactive Contact | 4.0 | All | All | All |
| Application | Avaya | Proactive Contact | 4.0 | All | All | All |
| Application | Avaya | Sip Enablement Services | - | All | All | All |
| Application | Avaya | Sip Enablement Services | 4.0 | All | All | All |
| Application | Avaya | Sip Enablement Services | - | All | All | All |

| | | | | | | |
|------------------|-----------|-------------------------------|------|-----|-----|-----|
| Application | Avaya | Sip Enablement Services | 4.0 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 6.06 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 7.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 7.10 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 8.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 6.06 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 7.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 7.10 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 8.04 | All | All | All |
| Operating System | Debian | Debian Linux | 4.0 | All | All | All |
| Operating System | Debian | Debian Linux | 4.0 | All | All | All |
| Operating System | Linux | Linux Kernel | All | All | All | All |
| Operating System | Linux | Linux Kernel | All | All | All | All |
| Operating System | Novell | Linux Desktop | 9 | All | All | All |
| Operating System | Novell | Linux Desktop | 9 | All | All | All |
| Operating System | Opensuse | Opensuse | 10.3 | All | All | All |
| Operating System | Opensuse | Opensuse | 11.0 | All | All | All |
| Operating System | Opensuse | Opensuse | 10.3 | All | All | All |
| Operating System | Opensuse | Opensuse | 11.0 | All | All | All |
| Operating System | Suse | Suse Linux Enterprise Desktop | 10 | sp1 | All | All |
| Operating System | Suse | Suse Linux Enterprise Desktop | 10 | sp2 | All | All |
| Operating System | Suse | Suse Linux Enterprise Desktop | 10 | sp1 | All | All |
| Operating System | Suse | Suse Linux Enterprise Desktop | 10 | sp2 | All | All |
| Operating System | Suse | Suse Linux Enterprise Server | 10 | sp1 | All | All |
| Operating System | Suse | Suse Linux Enterprise Server | 10 | sp2 | All | All |
| Operating System | Suse | Suse Linux Enterprise Server | 10 | sp1 | All | All |
| Operating System | Suse | Suse Linux Enterprise Server | 10 | sp2 | All | All |

References

| Reference | Source | Link |
|---|---------|---|
| [security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20 | SUSE | lists.opensuse.org |
| [security-announce] SUSE Security Summary Report: SUSE-SR:2008:025 | SUSE | lists.opensuse.org |
| Debian update for linux-2.6 - Secunia Advisories - Vulnerability Intelligence - Secunia.com | SECUNIA | secunia.com |
| ASA-2008-365 (RHSA-2008-0665) | CONFIRM | support.avaya.com |
| SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Intelligence - Secunia.com | SECUNIA | secunia.com |

| | | |
|---|---------|---|
| SUSE update for kernel - Secunia Advisories - Vulnerability Intelligence - Secunia.com | SECUNIA | secunia.com |
| Support | REDHAT | www.redhat.com |
| Red Hat update for kernel - Secunia Advisories - Vulnerability Intelligence - Secunia.com | SECUNIA | secunia.com |
| Repository / Oval Repository | OVAL | oval.cisecurity.org |
| Linux Kernel Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com | SECUNIA | secunia.com |
| [security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20 | SUSE | lists.opensuse.org |
| Red Hat update for kernel - Secunia Advisories - Vulnerability Intelligence - Secunia.com | SECUNIA | secunia.com |
| Ubuntu update for kernel - Secunia Advisories - Vulnerability Intelligence - Secunia.com | SECUNIA | secunia.com |
| [security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20 | SUSE | lists.opensuse.org |
| Linux Kernel TTY Operations NULL Pointer Dereference Denial of Service Vulnerabilities | BID | www.securityfocus.com |
| Security Advisory SA32103 - SUSE update for kernel - Secunia | SECUNIA | secunia.com |
| Webmail - OVH | VUPEN | www.vupen.com |
| oss-security - 2.6.25.10 security fixes, please assign CVE id | MLIST | www.openwall.com |
| [security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20 | SUSE | lists.opensuse.org |
| git.kernel.org | CONFIRM | git.kernel.org |
| Red Hat update for kernel - Secunia Advisories - Vulnerability Intelligence - Secunia.com | SECUNIA | secunia.com |
| git.kernel.org | MISC | git.kernel.org |
| SUSE update for kernel - Secunia Advisories - Vulnerability Intelligence - Secunia.com | SECUNIA | secunia.com |
| SUSE update for kernel - Secunia Advisories - Vulnerability Intelligence - Secunia.com | SECUNIA | secunia.com |
| Repository / Oval Repository | OVAL | oval.cisecurity.org |
| [security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20 | SUSE | lists.opensuse.org |
| Avaya Products Linux Kernel Multiple Vulnerabilities - Secunia.com | SECUNIA | secunia.com |
| USN-637-1: Linux kernel vulnerabilities Ubuntu security notices | UBUNTU | usn.ubuntu.com |
| 404: File not found | CONFIRM | kernel.org |
| Debian -- Security Information -- DSA-1630-1 linux-2.6 | DEBIAN | www.debian.org |
| [security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20 | SUSE | lists.opensuse.org |
| Support | REDHAT | www.redhat.com |
| Support | REDHAT | www.redhat.com |
| IBM X-Force Exchange | XF | exchange.xforce.ibmcloud.com |
| CVE Program record | CVE.ORG | www.cve.org |
| NVD vulnerability detail | NVD | nvd.nist.gov |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#)