



# CVE-2010-0307

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

|                        |                                                                                                                               |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2010-0307                                                                                                                 |
| <b>State</b>           | PUBLIC                                                                                                                        |
| <b>Assigner</b>        | secalert@redhat.com                                                                                                           |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                  |
| <b>Published</b>       | 2010-02-17 18:30:00 UTC                                                                                                       |
| <b>Updated</b>         | 2023-02-13 04:15:00 UTC                                                                                                       |
| <b>Description</b>     | The load_elf_binary function in fs/binfmt_elf.c in the Linux kernel before 2.6.32.8 on the x86_64 platform does not ensure th |

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                    | Product                      | Version | Update | Edition | Language |
|------------------|---------------------------|------------------------------|---------|--------|---------|----------|
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 6.06    | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 8.04    | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 8.10    | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 9.04    | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 9.10    | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 6.06    | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 8.04    | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 8.10    | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 9.04    | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 9.10    | All    | All     | All      |
| Operating System | <a href="#">Debian</a>    | <a href="#">Debian Linux</a> | 4.0     | All    | All     | All      |
| Operating System | <a href="#">Debian</a>    | <a href="#">Debian Linux</a> | 5.0     | All    | All     | All      |
| Operating System | <a href="#">Debian</a>    | <a href="#">Debian Linux</a> | 4.0     | All    | All     | All      |
| Operating System | <a href="#">Debian</a>    | <a href="#">Debian Linux</a> | 5.0     | All    | All     | All      |
| Operating System | <a href="#">Linux</a>     | <a href="#">Linux Kernel</a> | All     | All    | All     | All      |
| Operating System | <a href="#">Linux</a>     | <a href="#">Linux Kernel</a> | All     | All    | All     | All      |

| References                                                                        |          |                                                                          |              |
|-----------------------------------------------------------------------------------|----------|--------------------------------------------------------------------------|--------------|
| Reference                                                                         | Source   | Link                                                                     | Tags         |
| '[Security] DoS on x86_64' thread - MARC                                          | CONFIRM  | <a href="http://marc.info">marc.info</a>                                 | Mailing List |
| Support / Security / Advisories / / MDVSA-2010:066   Mandriva                     | MANDRIVA | <a href="http://www.mandriva.com">www.mandriva.com</a>                   | Third Party  |
| [security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20          | SUSE     | <a href="http://lists.opensuse.org">lists.opensuse.org</a>               | Mailing List |
| Bug 560547 – CVE-2010-0307 kernel: DoS on x86_64                                  | CONFIRM  | <a href="http://bugzilla.redhat.com">bugzilla.redhat.com</a>             | Issue Track  |
| oss-security - Re: CVE request - kernel: DoS on x86_64                            | MLIST    | <a href="http://www.openwall.com">www.openwall.com</a>                   | Mailing List |
| Vigil@nce: Linux kernel, denial of service on x86_64 - Global Security Mag Online | MISC     | <a href="http://www.globalsecuritymag.com">www.globalsecuritymag.com</a> | Third Party  |
| oss-security - Re: CVE request - kernel: DoS on x86_64                            | MLIST    | <a href="http://www.openwall.com">www.openwall.com</a>                   | Mailing List |
| SecurityFocus                                                                     | BUGTRAQ  | <a href="http://www.securityfocus.com">www.securityfocus.com</a>         | Third Party  |
| 404: File not found                                                               | CONFIRM  | <a href="http://www.kernel.org">www.kernel.org</a>                       | Vendor Adv   |
| Repository / Oval Repository                                                      | OVAL     | <a href="http://oval.cisecurity.org">oval.cisecurity.org</a>             | Third Party  |
| [SECURITY] Fedora 12 Update: kernel-2.6.31.12-174.2.19.fc12                       | FEDORA   | <a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a>     | Mailing List |
| VMSA-2011-0003                                                                    | CONFIRM  | <a href="http://www.vmware.com">www.vmware.com</a>                       | Third Party  |
| kernel/git/torvalds/linux.git - Linux kernel source tree                          | MISC     | <a href="http://git.kernel.org">git.kernel.org</a>                       |              |
| Red Hat update for kernel - Advisories - Community                                | SECUNIA  | <a href="http://secunia.com">secunia.com</a>                             | Third Party  |
| 'DoS on x86_64' - MARC                                                            | MLIST    | <a href="http://marc.info">marc.info</a>                                 | Mailing List |
| rhnl.redhat.com   Red Hat Support                                                 | REDHAT   | <a href="http://rhnl.redhat.com">rhnl.redhat.com</a>                     | Third Party  |
| rhnl.redhat.com   Red Hat Support                                                 | REDHAT   | <a href="http://www.redhat.com">www.redhat.com</a>                       | Third Party  |
| Ubuntu update for linux and linux-source-2.6.15 - Secunia.com                     | SECUNIA  | <a href="http://secunia.com">secunia.com</a>                             | Third Party  |
| Linux Kernel 64bit Personality Handling Local Denial of Service Vulnerability     | BID      | <a href="http://www.securityfocus.com">www.securityfocus.com</a>         | Exploit, Thi |
| Webmail- OVH                                                                      | VUPEN    | <a href="http://www.vupen.com">www.vupen.com</a>                         | Third Party  |
| kernel/git/torvalds/linux.git - Linux kernel source tree                          | CONFIRM  | <a href="http://git.kernel.org">git.kernel.org</a>                       | Vendor Adv   |
| USN-914-1: Linux kernel vulnerabilities   Ubuntu                                  | UBUNTU   | <a href="http://www.ubuntu.com">www.ubuntu.com</a>                       | Third Party  |
| ASA-2010-144 (RHSA-2010-0398)                                                     | CONFIRM  | <a href="http://support.avaya.com">support.avaya.com</a>                 | Third Party  |
| Vigil@nce: Linux kernel, denial of service on x86_64 - Global Security Mag Online | MISC     | <a href="http://www.globalsecuritymag.com">www.globalsecuritymag.com</a> |              |
| VMware ESX Server Multiple Kernel Vulnerabilities - Advisories - Community        | SECUNIA  | <a href="http://secunia.com">secunia.com</a>                             | Third Party  |
| oss-security - Re: CVE request - kernel: DoS on x86_64                            | MLIST    | <a href="http://www.openwall.com">www.openwall.com</a>                   | Mailing List |
| Debian update for linux-2.6 - Advisories - Community                              | SECUNIA  | <a href="http://secunia.com">secunia.com</a>                             | Third Party  |
| Support                                                                           | REDHAT   | <a href="http://www.redhat.com">www.redhat.com</a>                       | Third Party  |
| oss-security - CVE request - kernel: DoS on x86_64                                | MLIST    | <a href="http://www.openwall.com">www.openwall.com</a>                   | Mailing List |
| SUSE update for kernel - Advisories - Community                                   | SECUNIA  | <a href="http://secunia.com">secunia.com</a>                             | Third Party  |
| Debian -- Security Information -- DSA-1996-1 linux-2.6                            | DEBIAN   | <a href="http://www.debian.org">www.debian.org</a>                       | Third Party  |
| CVE Program record                                                                | CVE.ORG  | <a href="http://www.cve.org">www.cve.org</a>                             | canonical    |
| NVD vulnerability detail                                                          | NVD      | <a href="http://nvd.nist.gov">nvd.nist.gov</a>                           | canonical, c |

## Vendor Comments And Credit

| Organization | Published | Contributor | Statement |
|--------------|-----------|-------------|-----------|
|--------------|-----------|-------------|-----------|

|         |            |               |                                                                                                                                              |
|---------|------------|---------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| Red Hat | 2010-03-17 | Vincent Danen | Red Hat is aware of this issue and is tracking it via the following bug: <a href="https://bugzilla.redhat.co">https://bugzilla.redhat.co</a> |
|---------|------------|---------------|----------------------------------------------------------------------------------------------------------------------------------------------|

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](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)