# CVE-2007-3731

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2007-3731 |
| **State** | PUBLIC |
| **Assigner** | secalert@redhat.com |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2007-09-17 17:17:00 UTC |
| **Updated** | 2023-02-13 02:18:00 UTC |
| **Description** | The Linux kernel 2.6.20 and 2.6.21 does not properly handle an invalid LDT segment selector in %cs (the xcs field) during p |

## Risk And Classification

**Problem Types:** CWE-20

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Operating System | Linux | Linux Kernel | 2.6.20 | All | All | All |
| Operating System | Linux | Linux Kernel | 2.6.21 | All | All | All |
| Operating System | Linux | Linux Kernel | 2.6.20 | All | All | All |
| Operating System | Linux | Linux Kernel | 2.6.21 | All | All | All |

## References

| Reference | Source | Link | Tags |
|---|---|---|---|
| kernel/git/torvalds/linux.git - Linux kernel source tree | CONFIRM | git.kernel.org | |
| Linux Kernel ptrace Single Step "CS" Null Pointer Dereference - Advisories - Secunia | SECUNIA | secunia.com | |
| 8765 – NULL pointer dereference triggered by ptrace | MISC | bugzilla.kernel.org | Exploit |
| rPath update for kernel - Advisories - Secunia | SECUNIA | secunia.com | |
| kernel/git/torvalds/linux.git - Linux kernel source tree | MISC | git.kernel.org | |
| Debian update for kernel - Advisories - Secunia | SECUNIA | secunia.com | |
| 37286 | OSVDB | osvdb.org | |
| issues.rpath.com/browse/RPL-2304 | CONFIRM | issues.rpath.com | |
| rhn.redhat.com \| Red Hat Support | REDHAT | www.redhat.com | |
| SecurityFocus | BUGTRAQ | www.securityfocus.com | |

| | | | |
|---|---|---|---|
| access.redhat.com \| CVE-2007-3731 | MISC | access.redhat.com | |
| Repository / Oval Repository | OVAL | oval.cisecurity.org | |
| About Secunia Research \| Flexera | SECUNIA | secunia.com | |
| Linux Kernel PTrace NULL Pointer Dereference Local Denial Of Service Vulnerability | BID | www.securityfocus.com | |
| Ubuntu update for kernel - Advisories - Secunia | SECUNIA | secunia.com | |
| kernel/git/torvalds/linux.git - Linux kernel source tree | CONFIRM | git.kernel.org | |
| kernel/git/torvalds/linux.git - Linux kernel source tree | MISC | git.kernel.org | |
| Bug 248324 – CVE-2007-3731 NULL pointer dereference triggered by ptrace | CONFIRM | bugzilla.redhat.com | Patch |
| Red Hat Customer Portal | MISC | access.redhat.com | |
| Debian -- Security Information -- DSA-1378-2 linux-2.6 | DEBIAN | www.debian.org | |
| USN-518-1: Linux kernel vulnerabilities \| Ubuntu | UBUNTU | www.ubuntu.com | |
| Advisories:rPSA-2008-0094 - rPath Wiki | CONFIRM | wiki.rpath.com | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, ana |

## Vendor Comments And Credit

| Organization | Published | Contributor | Statement |
|---|---|---|---|
| Red Hat | 2007-10-18 | Mark J Cox | This issue did not affect the versions of the Linux kernel as shipped with Red Hat Enterprise Linu |

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 registred 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**