



CVE-2008-4226

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2008-4226 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2008-11-25 23:30:00 UTC |
| Updated | 2017-09-29 01:32:00 UTC |
| Description | Integer overflow in the xmlSAX2Characters function in libxml2 2.7.2 allows context-dependent attackers to cause a denial of |

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|---------|---------|---------|--------|---------|----------|
| Application | Xmlsoft | Libxml | 2.7.2 | All | All | All |
| Application | Xmlsoft | Libxml | 2.7.2 | All | All | All |

References

Reference

- rPath update for libxml2 - Secunia.com
- APPLE-SA-2009-06-17-1 iPhone OS 3.0 Software Update
- Bug 470466 – CVE-2008-4226 libxml2: integer overflow leading to memory corruption in xmlSAX2Characters
- sunsolve.sun.com/search/document.do
- Ubuntu update for libxml2 - Secunia Advisories - Vulnerability Intelligence - Secunia.com
- Fedora update for libxml2 - Secunia.com
- ASA-2009-002 (RHSA-2008-0988)
- [SECURITY] Fedora 9 Update: libxml2-2.7.2-2.fc9
- Slackware update for libxml2 - Secunia.com
- Webmail | OVH- OVH
- Repository / Oval Repository
- 251406

| |
|---|
| Sun Solaris libxml2 Two Integer Overflow Vulnerabilities - Secunia.com |
| 265329 |
| VMware ESX Server update for net-snmp and libxml2 - Secunia Advisories - Vulnerability Intelligence - Secunia.com |
| Libxml2 Two Integer Overflow Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com |
| Sun Java System Access Manager Policy Agent XML Processing Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com |
| Support / Security / Advisories // MDVSA-2008:231 Mandriva |
| The Slackware Linux Project: Slackware Security Advisories |
| SUSE Update for Multiple Packages - Secunia.com |
| 261688 |
| ASA-2009-067 (SUN 251406) |
| Advisories:rPSA-2008-0325 - rPath Wiki |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH |
| Gentoo update for libxml2 - Secunia Advisories - Vulnerability Intelligence - Secunia.com |
| Apple Safari Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com |
| sunsolve.sun.com/search/document.do |
| Libxml2 Integer Overflow in xmlSAX2Characters() May Let Remote Users Execute Arbitrary Code - SecurityTracker |
| HPSBMA02492 SSRT100079 rev.1 - HP System Management Homepage (SMH) for Linux and Windows, Remote Cross Site Scripting (XSS) |
| APPLE-SA-2009-06-08-1 Safari 4.0 |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH |
| Avaya CMS / IR Solaris libxml2 Integer Overflow Vulnerabilities - Secunia.com |
| Repository / Oval Repository |
| libxml2 'xmlSAX2Characters()' Integer Overflow Vulnerability |
| Debian update for libxml2 - Secunia.com |
| USN-673-1: libxml2 vulnerabilities Ubuntu |
| Webmail OVH- OVH |
| Sun Java System Access Manager XML Processing Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com |
| Support |
| Debian -- Security Information -- DSA-1666-1 libxml2 |
| About the security content of iPhone OS 3.0 Software Update |
| About the security content of Safari 4.0 |
| Repository / Oval Repository |
| admin.fedoraproject.org/updates/libxml2-2.7.2-2.fc10 |
| admin.fedoraproject.org/updates/libxml2-2.7.2-2.fc9 |
| [SECURITY] Fedora 8 Update: libxml2-2.7.2-2.fc8 |
| Webmail - OVH |
| 14101 0000 0001 1411 |

49993

libxml2: Multiple vulnerabilities — Gentoo Linux Documentation

Avaya Products Libxml2 Integer Overflow Vulnerabilities - Secunia.com

[security-announce] SUSE Security Summary Report: SUSE-SR:2008:026

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Red Hat update for libxml2 - Secunia.com

CVE Program record

NVD vulnerability detail



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](#)