



CVE-2008-4225

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

Summary

CVE	CVE-2008-4225
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 xmlBufferResize function in libxml2 2.7.2 allows context-dependent attackers to cause a denial of se

Risk And Classification

Problem Types: CWE-189

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
- 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
- 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

libxml2 'xmlBufferResize()' Remote Denial of Service Vulnerability

Support / Security / Advisories // MDVSA-2008:231 | Mandriva

49992

The Slackware Linux Project: Slackware Security Advisories

261688

ASA-2009-067 (SUN 251406)

Advisories:rPSA-2008-0325 - rPath Wiki

Bug 470480 – CVE-2008-4225 libxml2: integer overflow leading to infinite loop in xmlBufferResize

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Gentoo update for libxml2 - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Repository / Oval Repository

Libxml2 Integer Overflow in xmlBufferResize() Lets Remote Users Deny Service - SecurityTracker

Apple Safari Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com

sunsolve.sun.com/search/document.do

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

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

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

VMSA-2009-0001 - VMware

Repository / Oval Repository

libxml2: Multiple vulnerabilities — Gentoo Linux Documentation

Avaya Products Libxml2 Integer Overflow Vulnerabilities - Secunia.com

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](#)