CVE-2008-3529

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

Summary

CVE	CVE-2008-3529
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-09-12 16:56:00 UTC
Updated	2023-02-13 02:19:00 UTC
Description	Heap-based buffer overflow in the xmlParseAttValueComplex function in parser.c in libxml2 before 2.7.0 allows context-dep

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Iphone Os	All	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All
Operating System	Apple	Mac Os X	10.5.7	All	All	All
Application	Apple	Safari	All	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	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	8.04	All	All	All
Operating System	Canonical	Ubuntu Linux	8.10	All	All	All
Operating System	Canonical	Ubuntu Linux	9.04	All	All	All
Operating System	Debian	Debian Linux	4.0	All	All	All
Application	Xmlsoft	Libxml2	All	All	All	All
Application	Xmlsoft	Libxml2	2.4.30	All	All	All
Application	Xmlsoft	Libxml2	2.5.7	All	All	All
Application	Xmlsoft	Libxml2	2.5.8	All	All	All

Application	Xmlsoft	Libxml2	2.6.11	All	All	All
Application	Xmlsoft	Libxml2	2.6.13	All	All	All
Application	Xmlsoft	Libxml2	2.6.14	All	All	All
Application	Xmlsoft	Libxml2	2.6.16	All	All	All
Application	Xmlsoft	Libxml2	2.6.17	All	All	All
Application	Xmlsoft	Libxml2	2.6.18	All	All	All
Application	Xmlsoft	Libxml2	2.6.20	All	All	All
Application	Xmlsoft	Libxml2	2.6.22	All	All	All
Application	Xmlsoft	Libxml2	2.6.27	All	All	All
Application	Xmlsoft	Libxml2	2.6.6	All	All	All
Application	Xmlsoft	Libxml2	2.6.9	All	All	All
Application	Xmlsoft	Libxml2	2.4.30	All	All	All
Application	Xmlsoft	Libxml2	2.5.7	All	All	All
Application	Xmlsoft	Libxml2	2.5.8	All	All	All
Application	Xmlsoft	Libxml2	2.6.11	All	All	All
Application	Xmlsoft	Libxml2	2.6.13	All	All	All
Application	Xmlsoft	Libxml2	2.6.14	All	All	All
Application	Xmlsoft	Libxml2	2.6.16	All	All	All
Application	Xmlsoft	Libxml2	2.6.17	All	All	All
Application	Xmlsoft	Libxml2	2.6.18	All	All	All
Application	Xmlsoft	Libxml2	2.6.20	All	All	All
Application	Xmlsoft	Libxml2	2.6.22	All	All	All
Application	Xmlsoft	Libxml2	2.6.27	All	All	All
Application	Xmlsoft	Libxml2	2.6.6	All	All	All
Application	Xmlsoft	Libxml2	2.6.9	All	All	All
Application	Xmlsoft	Libxml2	All	All	All	All

References

Reference
rPath update for libxml2 - Secunia.com
APPLE-SA-2009-06-17-1 iPhone OS 3.0 Software Update
Releases
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
sunsolve.sun.com/search/document.do
Support / Security / Advisories / / MDVSA-2008:192 | Mandriva

247346

Avaya Products libxml2 XML Entity Name Buffer Overflow Vulnerability - Secunia.com

ASA-2008-400 (RHSA-2008-0884)

Safari RSS feed:// Buffer Overflow via libxml2 Exploit PoC

[security-announce] SUSE Security Summary Report: SUSE-SR:2008:018

APPLE-SA-2009-05-12 Safari 3.2.3

libxml XML Entity Name Heap Buffer Overflow Vulnerability

Red Hat update for libxml2 - Secunia Advisories - Vulnerability Intelligence - Secunia.com

265329

access.redhat.com | CVE-2008-3529

Sun Java System Access Manager Policy Agent XML Processing Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com

SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Bug 461015 – CVE-2008-3529 libxml2: long entity name heap buffer overflow

261688

Advisories:rPSA-2008-0325 - rPath Wiki

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

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

Apple Mac OS X Security Update Fixes Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com

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

About the security content of Safari 3.2.3

sunsolve.sun.com/search/document.do

About the security content of Security Update 2009-002 / Mac OS X v10.5.7

US-CERT Technical Cyber Security Alert TA09-133A -- Apple Updates for Multiple Vulnerabilities

APPLE-SA-2009-06-08-1 Safari 4.0

Support | Red Hat

USN-815-1: libxml2 vulnerabilities | Ubuntu

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Debian -- Security Information -- DSA-1654-1 libxml2

Repository / Oval Repository

Red Hat update for libxml2 - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Support

Repository / Oval Repository

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

Libxml2 Two Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com

IBM X-Force Exchange
Sun Java System Access Manager XML Processing Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com
Red Hat Customer Portal
About the security content of iPhone OS 3.0 Software Update
Avaya CMS Solaris "libxml2" XML Processing Vulnerability - Secunia Advisories - Vulnerability Intelligence - Secunia.com
About the security content of Safari 4.0
Apple Safari Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com
Sun Solaris "libxml2" XML Processing Vulnerability - Secunia.com
ASA-2009-025 (SUN 247346)
USN-644-1: libxml2 vulnerabilities | Ubuntu security notices
libxml2: Multiple vulnerabilities — Gentoo Linux Documentation
Red Hat Customer Portal - Access to 24x7 support and knowledge
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Libxml2 Heap Overflow in xmlParseAttValueComplex() Lets Remote Users Execute Arbitrary Code - SecurityTracker
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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**