



# CVE-2015-7500

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

## Summary

<b>CVE</b>	CVE-2015-7500
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2015-12-15 21:59:00 UTC
<b>Updated</b>	2023-02-13 00:53:00 UTC
<b>Description</b>	The xmlParseMisc function in parser.c in libxml2 before 2.9.3 allows context-dependent attackers to cause a denial of servi

## Risk And Classification

### Problem Types: CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Apple</a>	<a href="#">Iphone Os</a>	All	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	All	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Tvos</a>	All	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Watchos</a>	All	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	15.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	15.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	15.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	15.10	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	7.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	7.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Application	<a href="#">Hp</a>	<a href="#">Icewall Federation Agent</a>	3.0	All	All	All

Application	Hp	IceWall Federation Agent	3.0	All	All	All
Application	Hp	IceWall File Manager	3.0	All	All	All
Application	Hp	IceWall File Manager	3.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Application	Xmlsoft	Libxml2	All	All	All	All

## References

Reference	Source
APPLE-SA-2016-03-21-2 watchOS 2.2	APPLE
APPLE-SA-2016-03-21-5 OS X El Capitan 10.11.4 and Security Update 2016-002	APPLE
Debian -- Security Information -- DSA-3430-1 libxml2	DEBIAN
RHSA-2015:2549	REDHAT
APPLE-SA-2016-03-21-3 tvOS 9.2	APPLE
Bug 1281943 – CVE-2015-7500 libxml2: Heap buffer overflow in xmlParseMisc	CONFIRM
openSUSE-SU-2016:0106-1: moderate: Security update for libxml2	SUSE
USN-2834-1: libxml2 vulnerabilities   Ubuntu	UBUNTU
Red Hat Customer Portal	MISC
Red Hat Customer Portal	MISC
About the security content of watchOS 2.2 - Apple Support	CONFIRM
About the security content of iOS 9.3 - Apple Support	CONFIRM
openSUSE-SU-2015:2372-1: moderate: Security update for libxml2	SUSE
'[security bulletin] HPSBGN03537 rev.1 - HPE IceWall Federation Agent and IceWall File Manager runnin' - MARC	HP
CVE-2015-7500 Fix memory access error due to incorrect entities boundaries (f1063fdb) · Commits · GNOME / libxml2 · GitLab	CONFIRM
CVE-2015-7500 - Red Hat Customer Portal	MISC
RHSA-2016:1089	REDHAT
Releases	CONFIRM
Oracle Linux Bulletin - October 2015	CONFIRM
RHSA-2015:2550	REDHAT
HP IceWall File Manager (CVE-2015-7500) - CVE Details	CONFIRM

libxml2: Multiple vulnerabilities (GLSA 201701-37) — Gentoo security	GENIOU
libxml2 CVE-2015-7500 Denial of Service Vulnerability	BID
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC
APPLE-SA-2016-03-21-1 iOS 9.3	APPLE
Document Display   HPE Support Center	CONFIRM
About the security content of OS X El Capitan v10.11.4 and Security Update 2016-002 - Apple Support	CONFIRM
About the security content of tvOS 9.2 - Apple Support	CONFIRM
Libxml2 Multiple Flaws Let Remote Users Deny Service and Cause Other Unspecified Impacts - SecurityTracker	SECTRACK
Oracle Solaris Bulletin - January 2016	CONFIRM
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#)