



# CVE-2015-8242

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2015-8242
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2015-12-15 21:59:00 UTC
<b>Updated</b>	2019-03-08 16:06:00 UTC
<b>Description</b>	The xmlSAX2TextNode function in SAX2.c in the push interface in the HTML parser in libxml2 before 2.9.3 allows context-c

## 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	Tvos	All	All	All	All
Operating System	Apple	Watchos	All	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Application	Hp	Icewall Federation Agent	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	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Hpc Node</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Hpc Node</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	6.0	All	All	All
Application	<a href="#">Xmlsoft</a>	<a href="#">Libxml2</a>	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
RHSA-2015:2549	REDHAT
APPLE-SA-2016-03-21-3 tvOS 9.2	APPLE
oss-security - Re: Buffer overflow in libxml2	MLIST
openSUSE-SU-2016:0106-1: moderate: Security update for libxml2	SUSE
USN-2834-1: libxml2 vulnerabilities   Ubuntu	UBUNTU
oss-security - Buffer overflow in libxml2	MLIST
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
Bug 1281950 – CVE-2015-8242 libxml2: Buffer overread with HTML parser in push mode in xmlSAX2TextNode	CONFIRM
'[security bulletin] HPSBGN03537 rev.1 - HPE IceWall Federation Agent and IceWall File Manager runnin' - MARC	HP
RHSA-2016:1089	REDHAT
Releases	CONFIRM
Oracle Linux Bulletin - October 2015	CONFIRM
RHSA-2015:2550	REDHAT
libxml2: Multiple vulnerabilities (GLSA 201701-37) — Gentoo security	GENTOO
Bug 756372 – Buffer overread with HTML parser in push mode in xmlSAX2TextNode, causes segfault when compiled with ASAN	CONFIRM
APPLE-SA-2016-03-21-1 iOS 9.3	APPLE
CVE-2015-8242 Buffer overread with HTML parser in push mode (8fb4a770) · Commits · GNOME / libxml2 · GitLab	CONFIRM
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 - Security Tracker	SECURITY
libxml2 Out of Bounds Read Multiple Information Disclosure Vulnerabilities	BID
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](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)