



# CVE-2015-8317

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

## Summary

<b>CVE</b>	CVE-2015-8317
<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>	2017-09-14 01:29:00 UTC
<b>Description</b>	The xmlParseXMLDecl function in parser.c in libxml2 before 2.9.3 allows context-dependent attackers to obtain sensitive in

## 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="#">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	<a href="#">Hp</a>	<a href="#">Icewall Federation Agent</a>	3.0	All	All	All
Application	<a href="#">Hp</a>	<a href="#">Icewall File Manager</a>	3.0	All	All	All
Application	<a href="#">Hp</a>	<a href="#">Icewall File Manager</a>	3.0	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 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	Link
About the security content of iCloud for Windows 5.2.1 - Apple Support	CONFIRM	<a href="#">support.apple.com</a>
About the security content of OS X El Capitan v10.11.6 and Security Update 2016-004 - Apple Support	CONFIRM	<a href="#">support.apple.com</a>
oss-security - Libxml2: Several out of bounds reads	MLIST	<a href="#">www.openwall.com</a>
Debian -- Security Information -- DSA-3430-1 libxml2	DEBIAN	<a href="#">www.debian.org</a>
RHSA-2015:2549	REDHAT	<a href="#">rhn.redhat.com</a>
APPLE-SA-2016-07-18-1 OS X El Capitan v10.11.6 and Security Update 2016-004	APPLE	<a href="#">lists.apple.com</a>
APPLE-SA-2016-07-18-6 iTunes 12.4.2	APPLE	<a href="#">lists.apple.com</a>
Bug 1281930 – CVE-2015-8317 libxml2: Out-of-bounds heap read when parsing file with unfinished xml declaration	CONFIRM	<a href="#">bugzilla.redhat.com</a>
Apple iTunes APPLE-SA-2016-07-18-6 Multiple Memory Corruption Vulnerabilities	BID	<a href="#">www.securityfocus.com</a>
openSUSE-SU-2016:0106-1: moderate: Security update for libxml2	SUSE	<a href="#">lists.opensuse.org</a>
USN-2834-1: libxml2 vulnerabilities   Ubuntu	UBUNTU	<a href="#">www.ubuntu.com</a>
oss-security - Re: Libxml2: Several out of bounds reads	MLIST	<a href="#">www.openwall.com</a>
About the security content of watchOS 2.2.2 - Apple Support	CONFIRM	<a href="#">support.apple.com</a>
openSUSE-SU-2015:2372-1: moderate: Security update for libxml2	SUSE	<a href="#">lists.opensuse.org</a>
Fail parsing early on if encoding conversion failed (709a9521) · Commits · GNOME / libxml2 · GitLab	CONFIRM	<a href="#">git.gnome.org</a>
'[security bulletin] HPSBGN03537 rev.1 - HPE IceWall Federation Agent and IceWall File Manager runnin' - MARC	HP	<a href="#">marc.info</a>
Do not process encoding values if the declaration if broken (9aa37588) · Commits · GNOME / libxml2 · GitLab	CONFIRM	<a href="#">git.gnome.org</a>
Libxml2: Several out of bounds reads   The Fuzzing Project	MISC	<a href="#">blog.fuzzingproject.com</a>
RHSA-2016:1089	REDHAT	<a href="#">rhn.redhat.com</a>
Oracle Linux Bulletin - October 2015	CONFIRM	<a href="#">www.oracle.com</a>
Bug 751631 – xmlParseXMLDecl: out of bounds heap read on 0xff char in xml declaration	CONFIRM	<a href="#">bugzilla.redhat.com</a>
About the security content of iOS 9.3.3 - Apple Support	CONFIRM	<a href="#">support.apple.com</a>
APPLE-SA-2016-07-18-3 watchOS 2.2.2	APPLE	<a href="#">lists.apple.com</a>
About the security content of iTunes 12.4.2 for Windows - Apple Support	CONFIRM	<a href="#">support.apple.com</a>
Apple iTunes APPLE-SA-2016-07-18-6 Multiple Memory Corruption Vulnerabilities	CONFIRM	<a href="#">support.apple.com</a>

Document Display   HPE Support Center	CONFIRM	<a href="#">h20566.v</a>
APPLE-SA-2016-07-18-4 tvOS 9.2.2	APPLE	<a href="#">lists.app</a>
Libxml2 Multiple Flaws Let Remote Users Deny Service and Cause Other Unspecified Impacts - SecurityTracker	SECTRACK	<a href="#">www.sec</a>
APPLE-SA-2016-07-18-2 iOS 9.3.3	APPLE	<a href="#">lists.app</a>
About the security content of tvOS 9.2.2 - Apple Support	CONFIRM	<a href="#">support.a</a>
Bug 751603 – xmlParseXMLDecl: out of bounds heap access if versionencoding="es and any UTF-8 got	CONFIRM	<a href="#">bugzilla.c</a>
libxml2 Out of Bounds Read Multiple Information Disclosure Vulnerabilities	BID	<a href="#">www.sec</a>
Oracle Solaris Bulletin - January 2016	CONFIRM	<a href="#">www.ora</a>
CVE Program record	CVE.ORG	<a href="#">www.cve</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.c</a>

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](#)