



# CVE-2015-8241

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

## Summary

<b>CVE</b>	CVE-2015-8241
<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 xmlNextChar function in libxml2 2.9.2 does not properly check the state, which allows context-dependent attackers to c

## 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
Debian -- Security Information -- DSA-3430-1 libxml2	DEBIAN	<a href="http://www.debian.org">www.deb</a>
RHSA-2015:2549	REDHAT	<a href="http://rhn.redhat.com">rhn.redha</a>
oss-security - Re: Buffer overflow in libxml2	MLIST	<a href="http://www.openwall.com">www.ope</a>
openSUSE-SU-2016:0106-1: moderate: Security update for libxml2	SUSE	<a href="http://lists.opensuse.org">lists.open</a>
USN-2834-1: libxml2 vulnerabilities   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubu</a>
oss-security - Buffer overflow in libxml2	MLIST	<a href="http://www.openwall.com">www.ope</a>
Avoid extra processing of MarkupDecl when EOF (ab2b9a93) · Commits · GNOME / libxml2 · GitLab	CONFIRM	<a href="https://git.gnome.org">git.gnome</a>
openSUSE-SU-2015:2372-1: moderate: Security update for libxml2	SUSE	<a href="http://lists.opensuse.org">lists.open</a>
'[security bulletin] HPSBGN03537 rev.1 - HPE IceWall Federation Agent and IceWall File Manager runnin' - MARC	HP	<a href="http://marc.info">marc.info</a>
RHSA-2016:1089	REDHAT	<a href="http://rhn.redhat.com">rhn.redha</a>
Oracle Linux Bulletin - October 2015	CONFIRM	<a href="http://www.oracle.com">www.orac</a>
RHSA-2015:2550	REDHAT	<a href="http://rhn.redhat.com">rhn.redha</a>
Libxml2 'parser.c' Buffer Overflow Vulnerability	BID	<a href="http://www.securityfocus.com">www.seci</a>
Bug 1281936 – CVE-2015-8241 libxml2: Buffer overread with XML parser in xmlNextChar	CONFIRM	<a href="https://bugzilla.redhat.com">bugzilla.r</a>
Document Display   HPE Support Center	CONFIRM	<a href="http://h20566.www2.hp.com">h20566.w</a>
Libxml2 Multiple Flaws Let Remote Users Deny Service and Cause Other Unspecified Impacts - SecurityTracker	SECTRACK	<a href="http://www.securitytracker.com">www.seci</a>
Bug 756263 – Buffer overread with XML parser in xmlNextChar, causes segfault when compiled with ASAN	CONFIRM	<a href="https://bugzilla.gnome.org">bugzilla.g</a>
Oracle Solaris Bulletin - January 2016	CONFIRM	<a href="http://www.oracle.com">www.orac</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.g</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](#).

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