



# CVE-2015-7499

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

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2015-7499  |
| <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>     | Heap-based buffer overflow in the xmlGROW function in parser.c in libxml2 before 2.9.3 allows context-dependent attacker |

## 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 | Opensuse | Leap                         | 42.1 | All | All | All |
| Operating System | Opensuse | Leap                         | 42.1 | All | All | All |
| Operating System | Opensuse | Opensuse                     | 13.1 | All | All | All |
| Operating System | Opensuse | Opensuse                     | 13.2 | All | All | All |
| Operating System | Opensuse | Opensuse                     | 13.1 | All | All | All |
| Operating System | Opensuse | Opensuse                     | 13.2 | 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  | Link                                |
|--|---------|-------------------------------------|
| APPLE-SA-2016-03-21-2 watchOS 2.2  | APPLE   | <a href="#">lists.apple.com</a>     |
| APPLE-SA-2016-03-21-5 OS X El Capitan 10.11.4 and Security Update 2016-002 | APPLE   | <a href="#">lists.apple.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-2016-03-21-3 tvOS 9.2   | APPLE   | <a href="#">lists.apple.com</a>     |
| Detect incoherency on GROW (35bcb1d7) · Commits · GNOME / libxml2 · GitLab | CONFIRM | <a href="#">git.gnome.org</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>      |
| Red Hat Customer Portal  | MISC    | <a href="#">access.redhat.com</a>   |
| Red Hat Customer Portal  | MISC    | <a href="#">access.redhat.com</a>   |
| About the security content of watchOS 2.2 - Apple Support                  | CONFIRM | <a href="#">support.apple.com</a>   |
| About the security content of iOS 9.3 - 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>  |
| Bug 1281925 – CVE-2015-7499 libxml2: Heap-based buffer overflow in xmlGROW | CONFIRM | <a href="#">bugzilla.redhat.com</a> |
| libxml2: CVE-2015-7499: Heap-based buffer overflow in xmlGROW              | CONFIRM | <a href="#">bugzilla.redhat.com</a> |

|   |          |  |
|---|----------|--|
| Libxml2 'xmlGROW()' Function Denial of Service Vulnerability  | BID      | <a href="http://www.secdatabase.com">www.secdatabase.com</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.redhat.com</a>                   |
| Releases  | CONFIRM  | <a href="http://xmlsoft.org">xmlsoft.org</a>                         |
| Oracle Linux Bulletin - October 2015  | CONFIRM  | <a href="http://www.oracle.com">www.oracle.com</a>                   |
| RHSA-2015:2550  | REDHAT   | <a href="http://rhn.redhat.com">rhn.redhat.com</a>                   |
| libxml2: Multiple vulnerabilities (GLSA 201701-37) — Gentoo security  | GENTOO   | <a href="http://security.gentoo.org">security.gentoo.org</a>         |
| CVE-2015-7499 - Red Hat Customer Portal   | MISC     | <a href="http://access.redhat.com">access.redhat.com</a>             |
| Red Hat Customer Portal - Access to 24x7 support and knowledge  | MISC     | <a href="http://access.redhat.com">access.redhat.com</a>             |
| APPLE-SA-2016-03-21-1 iOS 9.3   | APPLE    | <a href="http://lists.apple.com">lists.apple.com</a>                 |
| Document Display   HPE Support Center   | CONFIRM  | <a href="http://h20566.www2.hp.com">h20566.www2.hp.com</a>           |
| About the security content of OS X El Capitan v10.11.4 and Security Update 2016-002 - Apple Support           | CONFIRM  | <a href="http://support.apple.com">support.apple.com</a>             |
| About the security content of tvOS 9.2 - Apple Support  | CONFIRM  | <a href="http://support.apple.com">support.apple.com</a>             |
| Libxml2 Multiple Flaws Let Remote Users Deny Service and Cause Other Unspecified Impacts - SecurityTracker    | SECTRACK | <a href="http://www.securitytracker.com">www.securitytracker.com</a> |
| Add xmlHaltParser() to stop the parser (28cd9cb7) · Commits · GNOME / libxml2 · GitLab                        | CONFIRM  | <a href="http://git.gnome.org">git.gnome.org</a>                     |
| CVE Program record  | CVE.ORG  | <a href="http://www.cve.org">www.cve.org</a>                         |
| NVD vulnerability detail  | NVD      | <a href="http://nvd.nist.gov">nvd.nist.gov</a>                       |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](http://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](http://The MITRE Corporation) and the authoritative source of CVE content is [MITRE's CVE web site](http://MITRE's CVE web site). This site includes MITRE data granted under the following [license](http://license).

**CVE.report and Source URL Uptime Status** [status.cve.report](http://status.cve.report)