



# CVE-2015-3451

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

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2015-3451  |
| <b>State</b>           | PUBLIC   |
| <b>Assigner</b>        | cve@mitre.org  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2015-05-12 19:59:00 UTC  |
| <b>Updated</b>         | 2020-04-29 13:17:00 UTC  |
| <b>Description</b>     | The _clone function in XML::LibXML before 2.0119 does not properly set the expand_entities option, which allows remote a |

## Risk And Classification

**Problem Types:** CWE-611

## 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> | 14.10   | 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> | 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> | 14.10   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a>     | <a href="#">Ubuntu Linux</a> | 15.04   | 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      |
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>       | 20      | All    | All     | All      |
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>       | 21      | All    | All     | All      |
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>       | 20      | All    | All     | All      |
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>       | 21      | All    | All     | All      |
| Operating System | <a href="#">Opensuse</a>      | <a href="#">Opensuse</a>     | 13.1    | All    | All     | All      |

|                  |                                    |                            |      |     |     |     |
|------------------|------------------------------------|----------------------------|------|-----|-----|-----|
| Operating System | <a href="#">Opensuse</a>           | <a href="#">Opensuse</a>   | 13.2 | All | All | All |
| Operating System | <a href="#">Opensuse</a>           | <a href="#">Opensuse</a>   | 13.1 | All | All | All |
| Operating System | <a href="#">Opensuse</a>           | <a href="#">Opensuse</a>   | 13.2 | All | All | All |
| Application      | <a href="#">Xml-libxml Project</a> | <a href="#">Xml-libxml</a> | All  | All | All | All |

## References

| Reference  | Source   | Link  | Ta |
|--|----------|---|----|
| openSUSE-SU-2015:1506-1: moderate: Security update for perl-XML-LibXML   | SUSE     | <a href="https://lists.opensuse.org">lists.opensuse.org</a>           | TI |
| <a href="http://cpansearch.perl.org/src/SHLOMIF/XML-LibXML-2.0119/Changes">cpansearch.perl.org/src/SHLOMIF/XML-LibXML-2.0119/Changes</a> | CONFIRM  | <a href="http://cpansearch.perl.org">cpansearch.perl.org</a>          | R  |
| oss-security - Re: CVE request: Perl XML::LibXML   | MLIST    | <a href="http://www.openwall.com">www.openwall.com</a>                | M  |
| XXE  | CONFIRM  | <a href="http://bitbucket.org">bitbucket.org</a>                      | V  |
| mandriva.com   | MANDRIVA | <a href="http://www.mandriva.com">www.mandriva.com</a>                | B  |
| oss-security - CVE request: Perl XML::LibXML   | MLIST    | <a href="http://www.openwall.com">www.openwall.com</a>                | M  |
| Mageia Advisory: MGASA-2015-0199 - Updated perl-XML-LibXML packages fix CVE-2015-3451  | CONFIRM  | <a href="http://advisories.mageia.org">advisories.mageia.org</a>      | TI |
| Debian -- Security Information -- DSA-3243-1 libxml-libxml-perl  | DEBIAN   | <a href="http://www.debian.org">www.debian.org</a>                    | TI |
| [SECURITY] Fedora 21 Update: perl-XML-LibXML-2.0119-1.fc21   | FEDORA   | <a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a> | TI |
| Perl HTML::Template::Pro Module XML External Entity Injection vulnerability  | BID      | <a href="http://www.securityfocus.com">www.securityfocus.com</a>      | TI |
| [SECURITY] Fedora 20 Update: perl-XML-LibXML-2.0119-1.fc20   | FEDORA   | <a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a> | TI |
| USN-2592-1: XML::LibXML vulnerability   Ubuntu   | UBUNTU   | <a href="http://www.ubuntu.com">www.ubuntu.com</a>                    | TI |
| CVE Program record   | CVE.ORG  | <a href="http://www.cve.org">www.cve.org</a>                          | ca |
| NVD vulnerability detail   | NVD      | <a href="http://nvd.nist.gov">nvd.nist.gov</a>                        | ca |

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](https://status.cve.report)