



CVE-2016-5002

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary

CVE	CVE-2016-5002
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-10-27 18:29:00 UTC
Updated	2024-01-22 17:15:00 UTC
Description	XML external entity (XXE) vulnerability in the Apache XML-RPC (aka ws-xmlrpc) library 3.1.3, as used in Apache Archiva, a

Risk And Classification

Problem Types: CWE-611

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Xml-rpc	3.1.3	All	All	All
Application	Apache	Xml-rpc	3.1.3	All	All	All

References

Reference
Beware of ws-xmlrpc library in your Java App ~ Из крайности в безопасность
Apache XML-RPC: Multiple Vulnerabilities (GLSA 202401-26) — Gentoo security
oss-security - Vulnerabilities in Apache Archiva
Malformed Request
Red Hat Customer Portal
Apache Archiva Bugs in XML-RPC Library Let Remote Users Conduct Server-Side Request Forgery Attacks, Deny Service, and Potentially E
IBM X-Force Exchange
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

[355437](#) Amazon Linux Security Advisory for xmlrpc : ALAS2-2023-2089

© [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](#)