



# CVE-2015-1833

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

## Summary

<b>CVE</b>	CVE-2015-1833
<b>State</b>	PUBLISHED
<b>Assigner</b>	redhat
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2015-05-29 15:59:13 UTC
<b>Updated</b>	2026-05-06 22:30:45 UTC
<b>Description</b>	XML external entity (XXE) vulnerability in Apache Jackrabbit before 2.0.6, 2.2.x before 2.2.14, 2.4.x before 2.4.6, 2.6.x before

## Risk And Classification

**Primary CVSS:** v2.0 6.4 from nvd@nist.gov

AV:N/AC:L/Au:N/C:P/I:P/A:N

**Problem Types:** CWE-20 | n/a

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

None

AV:N/AC:L/Au:N/C:P/I:P/A:N

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Jackrabbit	2.10.0	All	All	All

Application	Apache	Jackrabbit	2.2.0	All	All	All
Application	Apache	Jackrabbit	2.2.1	All	All	All
Application	Apache	Jackrabbit	2.2.10	All	All	All
Application	Apache	Jackrabbit	2.2.11	All	All	All
Application	Apache	Jackrabbit	2.2.12	All	All	All
Application	Apache	Jackrabbit	2.2.13	All	All	All
Application	Apache	Jackrabbit	2.2.2	All	All	All
Application	Apache	Jackrabbit	2.2.4	All	All	All
Application	Apache	Jackrabbit	2.2.5	All	All	All
Application	Apache	Jackrabbit	2.2.7	All	All	All
Application	Apache	Jackrabbit	2.2.8	All	All	All
Application	Apache	Jackrabbit	2.2.9	All	All	All
Application	Apache	Jackrabbit	2.4.0	All	All	All
Application	Apache	Jackrabbit	2.4.1	All	All	All
Application	Apache	Jackrabbit	2.4.2	All	All	All
Application	Apache	Jackrabbit	2.4.3	All	All	All
Application	Apache	Jackrabbit	2.4.4	All	All	All
Application	Apache	Jackrabbit	2.4.5	All	All	All
Application	Apache	Jackrabbit	2.6.0	All	All	All
Application	Apache	Jackrabbit	2.6.1	All	All	All
Application	Apache	Jackrabbit	2.6.2	All	All	All
Application	Apache	Jackrabbit	2.6.3	All	All	All
Application	Apache	Jackrabbit	2.6.4	All	All	All
Application	Apache	Jackrabbit	2.6.5	All	All	All
Application	Apache	Jackrabbit	2.8.0	All	All	All
Application	Apache	Jackrabbit	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

### References

Reference	Source
Apache JackRabbit - WebDAV XML External Entity - Java webapps Exploit	af854a3a-2127-422b-91ae-364da266
Apache Jackrabbit CVE-2015-1833 XML External Entity Information Disclosure Vulnerability	af854a3a-2127-422b-91ae-364da266
404 Not Found	af854a3a-2127-422b-91ae-364da266
Jackrabbit WebDAV XXE Injection - Pocket Storm	af854a3a-2127-422b-91ae-364da266

Jackrabbit WebDAV XXE Injection ~ Packet Storm	af854a3a-2127-422b-91ae-364da266
[JCR-3883] Jackrabbit WebDAV bundle susceptible to XXE/XEE attack (CVE-2015-1833) - ASF JIRA	af854a3a-2127-422b-91ae-364da266
SecurityFocus	af854a3a-2127-422b-91ae-364da266
CVE-2015-1833 (Jackrabbit WebDAV XXE vulnerability)	af854a3a-2127-422b-91ae-364da266
Debian -- Security Information -- DSA-3298-1 jackrabbit	af854a3a-2127-422b-91ae-364da266
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[150423](#) Adobe Experience Manager: WebDAV Exposed

© [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](#)