



CVE-2014-0170

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2014-0170
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-09-30 14:55:00 UTC
Updated	2017-08-29 01:34:00 UTC
Description	Teiid before 8.4.3 and before 8.7 and Red Hat JBoss Data Virtualization 6.0.0 before patch 3 allows remote attackers to read

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jboss	Teiid	8.4	All	All	All
Application	Jboss	Teiid	8.4	All	All	All
Application	Jboss	Teiid	All	All	All	All
Application	Redhat	Jboss Data Virtualization	All	All	All	All

References

Reference

- IBM X-Force Exchange
- Security Advisory SA61530 - Red Hat update for Red Hat JBoss Data Virtualization - Secunia
- Red Hat Customer Portal
- Red Hat JBoss Data Virtualization XML External Entity Processing Flaw Lets Remote Users Read Files on the Target System - SecurityTrack
- Login server redirect
- CVE Program record
- NVD vulnerability detail

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](#)