

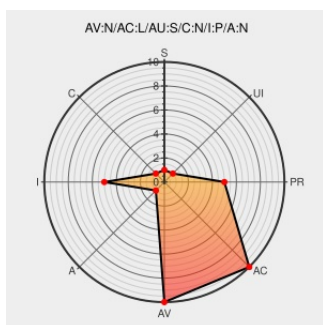


CVE-2014-7849

Published on: 02/13/2015 12:00:00 AM UTC

Last Modified on: 02/13/2023 12:08:09 AM UTC

CVE-2014-7849

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [JBoss Enterprise Application Platform](#) from [Redhat](#) contain the following vulnerability:

The Role Based Access Control (RBAC) implementation in JBoss Enterprise Application Platform (EAP) 6.2.0 through 6.3.2 does not properly verify authorization conditions, which allows remote authenticated users to add, modify, and undefine otherwise restricted attributes by leveraging the Maintainer role.

CVE-2014-7849 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **4 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

SINGLE

Confidentiality
Impact

NONE

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

Tags

Link

Red Hat Customer Portal

[Vendor Advisory](#)

[web.archive.org](#)

[text/html](#)

[Inactive Link](#) [Not Archived](#)

[REDHAT RHSA-2015:0216](#)

Red Hat Customer Portal

[Vendor Advisory](#)

[web.archive.org](#)

[text/html](#)

[Inactive Link](#) [Not Archived](#)

[REDHAT RHSA-2015:0218](#)

1165170 – (CVE-2014-7849) CVE-2014-7849 JBoss AS/WildFly Domain Management: Limited RBAC authorization bypass

[Vendor Advisory](#)

[bugzilla.redhat.com](#)

[text/html](#)

[CONFIRM](#)
[bugzilla.redhat.com/show_bug.cgi?id=1165170](#)

Red Hat Customer Portal

[Vendor Advisory](#)

[REDHAT RHSA-2015:0217](#)

web.archive.org[text/html](#)[Inactive Link](#) [Not Archived](#)

Red Hat JBoss Enterprise Application Platform Bugs Let Remote Users Obtain Potentially Sensitive Information and Remote Authenticated Users Bypass Security Controls - SecurityTracker

www.securitytracker.com[text/html](#) [SECTrack 1031741](#)

Red Hat Customer Portal

[Vendor Advisory](#)web.archive.org[text/html](#)[Inactive Link](#) [Not Archived](#) [REDHAT RHSA-2015:0215](#)[No Description Provided](#)[Vendor Advisory](#)rhn.redhat.com[Inactive Link](#) [Not Archived](#) [REDHAT RHSA-2015:0920](#)

IBM X-Force Exchange

exchange.xforce.ibmcloud.com[text/html](#) [XF redhat-jboss-cve20147849-sec-bypass\(100890\)](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Jboss Enterprise Application Platform	6.2.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	6.2.1	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	6.2.2	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	6.2.3	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	6.2.4	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	6.3.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	6.3.1	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	6.3.2	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	6.2.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	6.2.1	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	6.2.2	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	6.2.3	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	6.2.4	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	6.3.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	6.3.1	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	6.3.2	All	All	All

`cpe:2.3:a:redhat:jboss_enterprise_application_platform:6.2.0:*:*:*:*:*:`

cpe:2.3:a:redhat:jboss_enterprise_application_platform:6.2.1:*****:
cpe:2.3:a:redhat:jboss_enterprise_application_platform:6.2.2:*****:
cpe:2.3:a:redhat:jboss_enterprise_application_platform:6.2.3:*****:
cpe:2.3:a:redhat:jboss_enterprise_application_platform:6.2.4:*****:
cpe:2.3:a:redhat:jboss_enterprise_application_platform:6.3.0:*****:
cpe:2.3:a:redhat:jboss_enterprise_application_platform:6.3.1:*****:
cpe:2.3:a:redhat:jboss_enterprise_application_platform:6.3.2:*****:
cpe:2.3:a:redhat:jboss_enterprise_application_platform:6.2.0:*****:
cpe:2.3:a:redhat:jboss_enterprise_application_platform:6.2.1:*****:
cpe:2.3:a:redhat:jboss_enterprise_application_platform:6.2.2:*****:
cpe:2.3:a:redhat:jboss_enterprise_application_platform:6.2.3:*****:
cpe:2.3:a:redhat:jboss_enterprise_application_platform:6.2.4:*****:
cpe:2.3:a:redhat:jboss_enterprise_application_platform:6.3.0:*****:
cpe:2.3:a:redhat:jboss_enterprise_application_platform:6.3.1:*****:
cpe:2.3:a:redhat:jboss_enterprise_application_platform:6.3.2:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

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](#)