

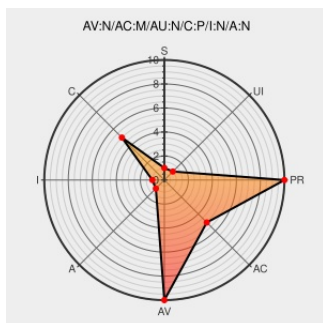


CVE-2012-4529

Published on: 10/28/2013 12:00:00 AM UTC

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

CVE-2012-4529

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

Certain versions of [Jboss Community Application Server](#) from [Redhat](#) contain the following vulnerability:

The `org.apache.catalina.connector.Response.encodeURL` method in Red Hat JBoss Web 7.1.x and earlier, when the tracking mode is set to COOKIE, sends the `jsessionId` in the URL of the first response of a session, which allows remote attackers to obtain the session id (1) via a man-in-the-middle attack or (2) by reading a log.

CVE-2012-4529 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

NONE

Availability
Impact

NONE

CVE References

Description

Tags

Link

Red Hat Customer Portal

[web.archive.org](#)

[text/html](#)

Inactive Link

Not Archived

[REDHAT RHSA-2013:0834](#)

Red Hat Customer Portal

[Vendor Advisory](#)

[web.archive.org](#)

[text/html](#)

Inactive Link

Not Archived

[REDHAT RHSA-2013:0833](#)

[JBWEB-249] Session Id is appended as URL path parameter even if disabled - Red Hat Issue Tracker

[issues.jboss.org](#)

[text/html](#)

[CONFIRM issues.jboss.org/browse/JBWEB-249](#)

Session Id is appended as URL path parameter in very first request | OCPsoft

[ocpsoft.org](#)

[text/html](#)

[MISC ocpsoft.org/support/topic/session-id-is-appended-as-url-path-parameter-in-very-first-request/](#)

Red Hat Customer Portal

Vendor Advisory

web.archive.org

text/html

Inactive Link

Not Archived

 REDHAT RHSA-2013:0839

Red Hat Customer Portal

Vendor Advisory

web.archive.org

text/html

Inactive Link

Not Archived

 REDHAT RHSA-2013:1437

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 Community Application Server	5.0.0	All	All	All
Application	Redhat	Jboss Community Application Server	5.0.1	All	All	All
Application	Redhat	Jboss Community Application Server	5.1.0	All	All	All
Application	Redhat	Jboss Community Application Server	6.0.0	All	All	All
Application	Redhat	Jboss Community Application Server	6.1.0	All	All	All
Application	Redhat	Jboss Community Application Server	7.0.0	All	All	All
Application	Redhat	Jboss Community Application Server	7.0.1	All	All	All
Application	Redhat	Jboss Community Application Server	7.0.2	All	All	All
Application	Redhat	Jboss Community Application Server	7.1.0	All	All	All
Application	Redhat	Jboss Community Application Server	5.0.0	All	All	All
Application	Redhat	Jboss Community Application Server	5.0.1	All	All	All
Application	Redhat	Jboss Community Application Server	5.1.0	All	All	All
Application	Redhat	Jboss Community Application Server	6.0.0	All	All	All
Application	Redhat	Jboss Community Application Server	6.1.0	All	All	All
Application	Redhat	Jboss Community Application Server	7.0.0	All	All	All
Application	Redhat	Jboss Community Application Server	7.0.1	All	All	All
Application	Redhat	Jboss Community Application Server	7.0.2	All	All	All
Application	Redhat	Jboss Community Application Server	7.1.0	All	All	All
Application	Redhat	Jboss Community Application Server	All	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	6.0.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	6.0.0	All	All	All

cpe:2.3:a:redhat:jboss_community_application_server:5.0.0:*:*:*:*:*:

