



CVE-2010-2474

Published on: 08/09/2010 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:13:18 AM UTC

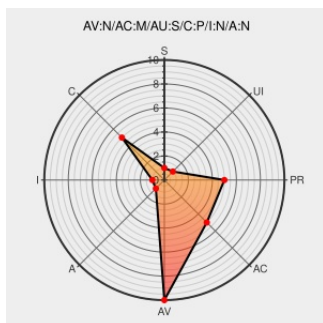
CVE-2010-2474

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

JBoss Enterprise Service Bus (ESB) before 4.7 CP02 in JBoss Enterprise SOA Platform before 5.0.2 does not properly consider the security domain with which a service is secured, which might allow remote attackers to gain privileges by executing a service.

CVE-2010-2474 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **3.5 - LOW**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

SINGLE

Confidentiality
Impact

PARTIAL

Integrity
Impact

NONE

Availability
Impact

NONE

CVE References

Description

Tags

Link

[#JBESB-3345] Security context should contain domain information - JBoss Issue Tracker

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

[CONFIRM jira.jboss.org/browse/JBESB-3345](#)

Bug 609442 – CVE-2010-2474 JBoss ESB privilege escalation in cross-domain contexts

[bugzilla.redhat.com](#)
[text/html](#)

[CONFIRM bugzilla.redhat.com/show_bug.cgi?id=609442](#)

JBoss ESB Domain Context Security Issue - Advisories - Community

[Vendor Advisory](#)
[web.archive.org](#)
[text/html](#)

[SECUNIA 40568](#)

Product Documentation - Red Hat Customer Portal

[www.redhat.com](#)
[text/html](#)

[CONFIRM www.redhat.com/docs/en-US/JBoss_SOA_Platform/5.0.2/html/5.0.2_Release_Notes/index.html](#)

JBoss Enterprise SOA Platform Multiple Security Issues - Advisories -

[Vendor Advisory](#)
[web.archive.org](#)

[SECUNIA 40681](#)

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 Service Bus	4.0	All	All	All
Application	Redhat	Jboss Enterprise Service Bus	4.2	All	All	All
Application	Redhat	Jboss Enterprise Service Bus	4.2.1	All	All	All
Application	Redhat	Jboss Enterprise Service Bus	4.3	All	All	All
Application	Redhat	Jboss Enterprise Service Bus	4.4	All	All	All
Application	Redhat	Jboss Enterprise Service Bus	4.5	All	All	All
Application	Redhat	Jboss Enterprise Service Bus	4.6	All	All	All
Application	Redhat	Jboss Enterprise Service Bus	4.0	All	All	All
Application	Redhat	Jboss Enterprise Service Bus	4.2	All	All	All
Application	Redhat	Jboss Enterprise Service Bus	4.2.1	All	All	All
Application	Redhat	Jboss Enterprise Service Bus	4.3	All	All	All
Application	Redhat	Jboss Enterprise Service Bus	4.4	All	All	All
Application	Redhat	Jboss Enterprise Service Bus	4.5	All	All	All
Application	Redhat	Jboss Enterprise Service Bus	4.6	All	All	All
Application	Redhat	Jboss Enterprise Service Bus	All	All	All	All
Application	Redhat	Jboss Enterprise Soa Platform	4.2.0	All	All	All
Application	Redhat	Jboss Enterprise Soa Platform	4.2.0	cp01	All	All
Application	Redhat	Jboss Enterprise Soa Platform	4.2.0	cp02	All	All
Application	Redhat	Jboss Enterprise Soa Platform	4.2.0	cp03	All	All
Application	Redhat	Jboss Enterprise Soa Platform	4.2.0	cp04	All	All
Application	Redhat	Jboss Enterprise Soa Platform	4.2.0	cp05	All	All
Application	Redhat	Jboss Enterprise Soa Platform	4.2.0	tp02	All	All
Application	Redhat	Jboss Enterprise Soa Platform	4.3.0	All	All	All
Application	Redhat	Jboss Enterprise Soa Platform	4.3.0	cp01	All	All
Application	Redhat	Jboss Enterprise Soa Platform	4.3.0	cp02	All	All
Application	Redhat	Jboss Enterprise Soa Platform	4.3.0	cp03	All	All
Application	Redhat	Jboss Enterprise Soa Platform	4.3.0	cp04	All	All

Application	Redhat	Jboss Enterprise Soa Platform	5.0.0	All	All	All
Application	Redhat	Jboss Enterprise Soa Platform	5.0.1	All	All	All
Application	Redhat	Jboss Enterprise Soa Platform	4.2.0	All	All	All
Application	Redhat	Jboss Enterprise Soa Platform	4.2.0	cp01	All	All
Application	Redhat	Jboss Enterprise Soa Platform	4.2.0	cp02	All	All
Application	Redhat	Jboss Enterprise Soa Platform	4.2.0	cp03	All	All
Application	Redhat	Jboss Enterprise Soa Platform	4.2.0	cp04	All	All
Application	Redhat	Jboss Enterprise Soa Platform	4.2.0	cp05	All	All
Application	Redhat	Jboss Enterprise Soa Platform	4.2.0	tp02	All	All
Application	Redhat	Jboss Enterprise Soa Platform	4.3.0	All	All	All
Application	Redhat	Jboss Enterprise Soa Platform	4.3.0	cp01	All	All
Application	Redhat	Jboss Enterprise Soa Platform	4.3.0	cp02	All	All
Application	Redhat	Jboss Enterprise Soa Platform	4.3.0	cp03	All	All
Application	Redhat	Jboss Enterprise Soa Platform	4.3.0	cp04	All	All
Application	Redhat	Jboss Enterprise Soa Platform	5.0.0	All	All	All
Application	Redhat	Jboss Enterprise Soa Platform	5.0.1	All	All	All
cpe:2.3:a:redhat:jboss_enterprise_service_bus:4.0:*****:						
cpe:2.3:a:redhat:jboss_enterprise_service_bus:4.2:*****:						
cpe:2.3:a:redhat:jboss_enterprise_service_bus:4.2.1:*****:						
cpe:2.3:a:redhat:jboss_enterprise_service_bus:4.3:*****:						
cpe:2.3:a:redhat:jboss_enterprise_service_bus:4.4:*****:						
cpe:2.3:a:redhat:jboss_enterprise_service_bus:4.5:*****:						
cpe:2.3:a:redhat:jboss_enterprise_service_bus:4.6:*****:						
cpe:2.3:a:redhat:jboss_enterprise_service_bus:4.0:*****:						
cpe:2.3:a:redhat:jboss_enterprise_service_bus:4.2:*****:						
cpe:2.3:a:redhat:jboss_enterprise_service_bus:4.2.1:*****:						
cpe:2.3:a:redhat:jboss_enterprise_service_bus:4.3:*****:						
cpe:2.3:a:redhat:jboss_enterprise_service_bus:4.4:*****:						
cpe:2.3:a:redhat:jboss_enterprise_service_bus:4.5:*****:						
cpe:2.3:a:redhat:jboss_enterprise_service_bus:4.6:*****:						
cpe:2.3:a:redhat:jboss_enterprise_service_bus:*****:						

cpe:2.3:a:redhat:jboss_enterprise_soa_platform:4.2.0:*****:
cpe:2.3:a:redhat:jboss_enterprise_soa_platform:4.2.0:cp01:*****:
cpe:2.3:a:redhat:jboss_enterprise_soa_platform:4.2.0:cp02:*****:
cpe:2.3:a:redhat:jboss_enterprise_soa_platform:4.2.0:cp03:*****:
cpe:2.3:a:redhat:jboss_enterprise_soa_platform:4.2.0:cp04:*****:
cpe:2.3:a:redhat:jboss_enterprise_soa_platform:4.2.0:cp05:*****:
cpe:2.3:a:redhat:jboss_enterprise_soa_platform:4.2.0:tp02:*****:
cpe:2.3:a:redhat:jboss_enterprise_soa_platform:4.3.0:*****:
cpe:2.3:a:redhat:jboss_enterprise_soa_platform:4.3.0:cp01:*****:
cpe:2.3:a:redhat:jboss_enterprise_soa_platform:4.3.0:cp02:*****:
cpe:2.3:a:redhat:jboss_enterprise_soa_platform:4.3.0:cp03:*****:
cpe:2.3:a:redhat:jboss_enterprise_soa_platform:4.3.0:cp04:*****:
cpe:2.3:a:redhat:jboss_enterprise_soa_platform:5.0.0:*****:
cpe:2.3:a:redhat:jboss_enterprise_soa_platform:5.0.1:*****:
cpe:2.3:a:redhat:jboss_enterprise_soa_platform:4.2.0:*****:
cpe:2.3:a:redhat:jboss_enterprise_soa_platform:4.2.0:cp01:*****:
cpe:2.3:a:redhat:jboss_enterprise_soa_platform:4.2.0:cp02:*****:
cpe:2.3:a:redhat:jboss_enterprise_soa_platform:4.2.0:cp03:*****:
cpe:2.3:a:redhat:jboss_enterprise_soa_platform:4.2.0:cp04:*****:
cpe:2.3:a:redhat:jboss_enterprise_soa_platform:4.2.0:cp05:*****:
cpe:2.3:a:redhat:jboss_enterprise_soa_platform:4.2.0:tp02:*****:
cpe:2.3:a:redhat:jboss_enterprise_soa_platform:4.3.0:*****:
cpe:2.3:a:redhat:jboss_enterprise_soa_platform:4.3.0:cp01:*****:
cpe:2.3:a:redhat:jboss_enterprise_soa_platform:4.3.0:cp02:*****:
cpe:2.3:a:redhat:jboss_enterprise_soa_platform:4.3.0:cp03:*****:
cpe:2.3:a:redhat:jboss_enterprise_soa_platform:4.3.0:cp04:*****:
cpe:2.3:a:redhat:jboss_enterprise_soa_platform:5.0.0:*****:
cpe:2.3:a:redhat:jboss_enterprise_soa_platform:5.0.1:*****:

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](#)