



CVE-2010-3862

Published on: 12/30/2010 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:13:17 AM UTC

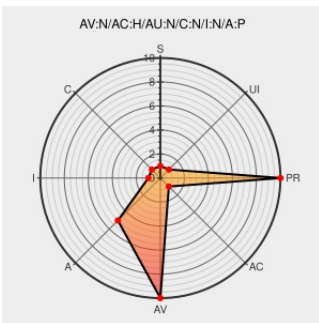
CVE-2010-3862

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

The

org.jboss.remoting.transport.bisocket.BisocketServerInvoker\$SecondaryServerSocketThread.r method in JBoss Remoting 2.2.x before 2.2.3.SP4 and 2.5.x before 2.5.3.SP2 in Red Hat JBoss Enterprise Application Platform (aka JBoss EAP or JBEAP) 4.3 through 4.3.0.CP09, and 5.1.0; and JBoss Enterprise Web Platform (aka JBEWP) 5.1.0; allows remote attackers to cause a denial of service (daemon outage) by establishing a bisocket control connection TCP session, and then not sending any application data.

CVE-2010-3862 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **2.6 - LOW**

Access
Vector

NETWORK

Access
Complexity

HIGH

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

rhn.redhat.com | Red Hat Support

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

[REDHAT RHSA-2010:0963](#)

rhn.redhat.com | Red Hat Support

[Vendor Advisory](#)
www.redhat.com

[REDHAT RHSA-2010:0961](#)

[text/html](#)[rhn.redhat.com](#) | Red Hat Support[Vendor Advisory](#)
[www.redhat.com](#)
[text/html](#) [REDHAT RHSA-2010:0938](#)[#JBREM-1261] Prevent DOS attack on
BisocketServerInvoker\$SecondaryServerSocketThread - JBoss Issue Tracker[issues.jboss.org](#)
[text/html](#) [CONFIRM](#)
[issues.jboss.org/browse/JBREM-1261](#)[rhn.redhat.com](#) | Red Hat Support[Vendor Advisory](#)
[www.redhat.com](#)
[text/html](#) [REDHAT RHSA-2010:0937](#)

Login server redirect

[issues.jboss.org](#)
[text/html](#) [MISC](#)
[issues.jboss.org/browse/JBPAPP-5253](#)[rhn.redhat.com](#) | Red Hat Support[Vendor Advisory](#)
[www.redhat.com](#)
[text/html](#) [REDHAT RHSA-2010:0939](#)[rhn.redhat.com](#) | Red Hat Support[Vendor Advisory](#)
[www.redhat.com](#)
[text/html](#) [REDHAT RHSA-2010:0959](#)SecurityTracker: JBoss Enterprise Application Platform Bugs Let Remote Users
Execute Arbitrary Code, Deny Service, and Conduct Cross-Site Request Forgery
Attacks[securitytracker.com](#)
[text/html](#) [SECTrack 1024813](#)[rhn.redhat.com](#) | Red Hat Support[Vendor Advisory](#)
[www.redhat.com](#)
[text/html](#) [REDHAT RHSA-2010:0962](#)

641389 – (CVE-2010-3862) CVE-2010-3862 JBoss Remoting Denial-Of-Service

[Patch](#)
[bugzilla.redhat.com](#)
[text/html](#) [CONFIRM](#)
[bugzilla.redhat.com/show_bug.cgi?id=641389](#)[rhn.redhat.com](#) | Red Hat Support[Vendor Advisory](#)
[www.redhat.com](#)
[text/html](#) [REDHAT RHSA-2010:0960](#)

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	4.3.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.3.0	cp01	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.3.0	cp02	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.3.0	cp03	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.3.0	cp04	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.3.0	cp05	All	All

Application	Redhat	Jboss Enterprise Application Platform	4.3.0	cp06	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.3.0	cp07	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.3.0	cp08	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.3.0	cp09	All	All
Application	Redhat	Jboss Enterprise Application Platform	5.1.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.3.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.3.0	cp01	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.3.0	cp02	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.3.0	cp03	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.3.0	cp04	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.3.0	cp05	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.3.0	cp06	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.3.0	cp07	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.3.0	cp08	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.3.0	cp09	All	All
Application	Redhat	Jboss Enterprise Application Platform	5.1.0	All	All	All
Application	Redhat	Jboss Enterprise Web Platform	5.1.0	All	All	All
Application	Redhat	Jboss Enterprise Web Platform	5.1.0	All	All	All
Application	Redhat	Jboss Remoting	2.2.0	All	All	All
Application	Redhat	Jboss Remoting	2.2.2	sp10	All	All
Application	Redhat	Jboss Remoting	2.2.2	sp11	All	All
Application	Redhat	Jboss Remoting	2.2.2	sp2	All	All
Application	Redhat	Jboss Remoting	2.2.2	sp4	All	All
Application	Redhat	Jboss Remoting	2.2.2	sp7	All	All
Application	Redhat	Jboss Remoting	2.2.2	sp8	All	All
Application	Redhat	Jboss Remoting	2.2.3	All	All	All
Application	Redhat	Jboss Remoting	2.2.3	sp1	All	All
Application	Redhat	Jboss Remoting	2.2.3	sp2	All	All
Application	Redhat	Jboss Remoting	2.2.3	sp3	All	All
Application	Redhat	Jboss Remoting	2.2.0	All	All	All
Application	Redhat	Jboss Remoting	2.2.2	sp10	All	All
Application	Redhat	Jboss Remoting	2.2.2	sp11	All	All
Application	Redhat	Jboss Remoting	2.2.2	sp2	All	All
Application	Redhat	Jboss Remoting	2.2.2	sp4	All	All
Application	Redhat	Jboss Remoting	2.2.2	sp7	All	All

Application	Redhat	Jboss Remoting	2.2.2	sp8	All	All
Application	Redhat	Jboss Remoting	2.2.3	All	All	All
Application	Redhat	Jboss Remoting	2.2.3	sp1	All	All
Application	Redhat	Jboss Remoting	2.2.3	sp2	All	All
Application	Redhat	Jboss Remoting	2.2.3	sp3	All	All
cpe:2.3:a:redhat:jboss_enterprise_application_platform:4.3.0:*:*:*:*:*:						
cpe:2.3:a:redhat:jboss_enterprise_application_platform:4.3.0:cp01:*:*:*:*:*:						
cpe:2.3:a:redhat:jboss_enterprise_application_platform:4.3.0:cp02:*:*:*:*:*:						
cpe:2.3:a:redhat:jboss_enterprise_application_platform:4.3.0:cp03:*:*:*:*:*:						
cpe:2.3:a:redhat:jboss_enterprise_application_platform:4.3.0:cp04:*:*:*:*:*:						
cpe:2.3:a:redhat:jboss_enterprise_application_platform:4.3.0:cp05:*:*:*:*:*:						
cpe:2.3:a:redhat:jboss_enterprise_application_platform:4.3.0:cp06:*:*:*:*:*:						
cpe:2.3:a:redhat:jboss_enterprise_application_platform:4.3.0:cp07:*:*:*:*:*:						
cpe:2.3:a:redhat:jboss_enterprise_application_platform:4.3.0:cp08:*:*:*:*:*:						
cpe:2.3:a:redhat:jboss_enterprise_application_platform:4.3.0:cp09:*:*:*:*:*:						
cpe:2.3:a:redhat:jboss_enterprise_application_platform:5.1.0:*:*:*:*:*:						
cpe:2.3:a:redhat:jboss_enterprise_application_platform:4.3.0:*:*:*:*:*:						
cpe:2.3:a:redhat:jboss_enterprise_application_platform:4.3.0:cp01:*:*:*:*:*:						
cpe:2.3:a:redhat:jboss_enterprise_application_platform:4.3.0:cp02:*:*:*:*:*:						
cpe:2.3:a:redhat:jboss_enterprise_application_platform:4.3.0:cp03:*:*:*:*:*:						
cpe:2.3:a:redhat:jboss_enterprise_application_platform:4.3.0:cp04:*:*:*:*:*:						
cpe:2.3:a:redhat:jboss_enterprise_application_platform:4.3.0:cp05:*:*:*:*:*:						
cpe:2.3:a:redhat:jboss_enterprise_application_platform:4.3.0:cp06:*:*:*:*:*:						
cpe:2.3:a:redhat:jboss_enterprise_application_platform:4.3.0:cp07:*:*:*:*:*:						
cpe:2.3:a:redhat:jboss_enterprise_application_platform:4.3.0:cp08:*:*:*:*:*:						
cpe:2.3:a:redhat:jboss_enterprise_application_platform:4.3.0:cp09:*:*:*:*:*:						
cpe:2.3:a:redhat:jboss_enterprise_application_platform:5.1.0:*:*:*:*:*:						
cpe:2.3:a:redhat:jboss_enterprise_web_platform:5.1.0:*:*:*:*:*:						
cpe:2.3:a:redhat:jboss_enterprise_web_platform:5.1.0:*:*:*:*:*:						
cpe:2.3:a:redhat:jboss_remoting:2.2.0:*:*:*:*:*:						

cpe:2.3:a:redhat:jboss_remoting:2.2.0:*:*:*:*:*:
cpe:2.3:a:redhat:jboss_remoting:2.2.2:sp10:*:*:*:*:*:
cpe:2.3:a:redhat:jboss_remoting:2.2.2:sp11:*:*:*:*:*:
cpe:2.3:a:redhat:jboss_remoting:2.2.2:sp2:*:*:*:*:*:
cpe:2.3:a:redhat:jboss_remoting:2.2.2:sp4:*:*:*:*:*:
cpe:2.3:a:redhat:jboss_remoting:2.2.2:sp7:*:*:*:*:*:
cpe:2.3:a:redhat:jboss_remoting:2.2.2:sp8:*:*:*:*:*:
cpe:2.3:a:redhat:jboss_remoting:2.2.3:*:*:*:*:*:
cpe:2.3:a:redhat:jboss_remoting:2.2.3:sp1:*:*:*:*:*:
cpe:2.3:a:redhat:jboss_remoting:2.2.3:sp2:*:*:*:*:*:
cpe:2.3:a:redhat:jboss_remoting:2.2.3:sp3:*:*:*:*:*:
cpe:2.3:a:redhat:jboss_remoting:2.2.0:*:*:*:*:*:
cpe:2.3:a:redhat:jboss_remoting:2.2.2:sp10:*:*:*:*:*:
cpe:2.3:a:redhat:jboss_remoting:2.2.2:sp11:*:*:*:*:*:
cpe:2.3:a:redhat:jboss_remoting:2.2.2:sp2:*:*:*:*:*:
cpe:2.3:a:redhat:jboss_remoting:2.2.2:sp4:*:*:*:*:*:
cpe:2.3:a:redhat:jboss_remoting:2.2.2:sp7:*:*:*:*:*:
cpe:2.3:a:redhat:jboss_remoting:2.2.2:sp8:*:*:*:*:*:
cpe:2.3:a:redhat:jboss_remoting:2.2.3:*:*:*:*:*:
cpe:2.3:a:redhat:jboss_remoting:2.2.3:sp1:*:*:*:*:*:
cpe:2.3:a:redhat:jboss_remoting:2.2.3:sp2:*:*:*:*:*:
cpe:2.3:a:redhat:jboss_remoting:2.2.3:sp3:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

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](#)