



CVE-2010-4265

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary

CVE	CVE-2010-4265
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-12-30 21:00:02 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The org.jboss.remoting.transport.bisocket.BisocketServerInvoker\$SecondaryServerSocketThread.run method in JBoss Remoting.jar has the following code: <pre>try { socket = new ServerSocket(port); while (true) { try { clientSocket = socket.accept(); new Thread(new SecondaryServerSocketThread(clientSocket, this)).start(); } catch (IOException e) { // ignore } } } catch (IOException e) { // ignore }</pre>

Risk And Classification

Primary CVSS: v2.0 2.6 from nvd@nist.gov

AV:N/AC:H/Au:N/C:N/I:N/A:P

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

High

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

AV:N/AC:H/Au:N/C:N/I:N/A:P

NVD Known Affected Configurations (CPE 2.3)

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 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

Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		

References						
Reference					Source	
Login server redirect					af854a3a-2127-422b	
JBoss Enterprise Application Platform Remoting Bug Lets Remote Users Deny Service - SecurityTracker					af854a3a-2127-422b	
rhn.redhat.com Red Hat Support					af854a3a-2127-422b	
660623 – (CVE-2010-4265) CVE-2010-4265 jboss-remoting: missing fix for CVE-2010-3862					af854a3a-2127-422b	
[#JBREM-1261] Prevent DOS attack on BisocketServerInvoker\$SecondaryServerSocketThread - JBoss Issue Tracker					af854a3a-2127-422b	
rhn.redhat.com Red Hat Support					af854a3a-2127-422b	
CVE Program record					CVE.ORG	
NVD vulnerability detail					NVD	

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)