



[MITRE](#)
[NVD](#)
[CVE.ORG](#)
[JSON API](#)
[Print: PDF](#)

CVE	CVE-2009-1380
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-12-15 18:30:00 UTC
Updated	2023-02-13 02:20:00 UTC
Description	Cross-site scripting (XSS) vulnerability in JMX-Console in JBossAs in Red Hat JBoss Enterprise Application Platform (aka JBoss EAP)

Problem Types: CWE-79

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Jboss Enterprise Application Platform	4.2	cp01	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.2	cp02	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.2	cp03	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.2.0	cp01	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.2.0	cp02	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.2.0	cp03	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.2.0	cp04	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.2.0	cp05	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.2.0	cp06	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.2.0	cp07	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.3	cp01	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	4.2	cp01	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.2	cp02	All	All

Application	Redhat	Jboss Enterprise Application Platform	4.2	cp03	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.2.0	cp01	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.2.0	cp02	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.2.0	cp03	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.2.0	cp04	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.2.0	cp05	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.2.0	cp06	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.2.0	cp07	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.3	cp01	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

References

Reference

rh.n.redhat.com | Red Hat Support

Red Hat Customer Portal - Access to 24x7 support and knowledge

Red Hat Customer Portal

Red Hat Customer Portal - Access to 24x7 support and knowledge

IBM X-Force Exchange

511224 – (CVE-2009-1380) CVE-2009-1380 jbossas JMX-Console cross-site-scripting in filter parameter

Red Hat Customer Portal - Access to 24x7 support and knowledge

SecurityTracker.com Archives - JBoss Enterprise Application Platform Input Validation Holes in the JMX Console and Web Console Permits C

rh.n.redhat.com | Red Hat Support

About Secunia Research | Flexera

JBoss Enterprise Application Platform Multiple Vulnerabilities

CVE-2009-1380 - Red Hat Customer Portal

rh.n.redhat.com | Red Hat Support

jira.jboss.org/jira/browse/JBPAPP-1983

rh.n.redhat.com | Red Hat Support

CVE Program record

NVD vulnerability detail

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](#)