



CVE-2010-0738

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

Summary

CVE	CVE-2010-0738
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-04-28 22:30:00 UTC
Updated	2026-04-22 14:37:41 UTC
Description	The JMX-Console web application in JBossAs in Red Hat JBoss Enterprise Application Platform (aka JBoss EAP or JBEAP)

Risk And Classification

Primary CVSS: v3.1 5.3 MEDIUM from nvd@nist.gov

CVSS: 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

EPSS: 0.915230000 probability, percentile 0.996770000 (date 2026-04-25)

CISA KEV: Listed on 2022-05-25; due 2022-06-15; ransomware use Known

Problem Types: NVD-CWE-noinfo | CWE-749 | n/a | CWE-749 CWE-749 Exposed Dangerous Method or Function

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
3.1	ADP	DECLARED	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
2.0	nvd@nist.gov	Primary	5		AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

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

CISA Known Exploited Vulnerability

Vendor	Red Hat
Product	JBoss
Name	Red Hat JBoss Authentication Bypass Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2010-0738

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Jboss Enterprise Application Platform	4.2.0	-	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.3.0	-	All	All

Vendor Declared Affected Products

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

References

Reference

IBM X-Force Exchange

[rhn.redhat.com | Red Hat Support](#)

Red Hat JBoss Enterprise Application Platform Three Security Issues - Advisories - Community

[rhn.redhat.com | Red Hat Support](#)

'[security bulletin] HPSBMU02714 SSRT100244 rev.2 - HP Network Node Manager i (NNMi) for HP-UX, Linux' - MARC

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

[www.cisa.gov/known-exploited-vulnerabilities-catalog](#)

Bug 574105 – CVE-2010-0738 JBoss EAP jmx authentication bypass with crafted HTTP request

JBoss Enterprise Application Platform Multiple Vulnerabilities

[rhn.redhat.com | Red Hat Support](#)

Vulnerability Report - JMX-Console in JBoss AS is vulnerable to attack

[rhn.redhat.com | Red Hat Support](#)

SecurityTracker.com Archives - JBoss Enterprise Application Platform Bugs Let Remote Users Bypass Authentication and Access Potentially

JBoss, JMX Console, misconfigured DeploymentScanner - SecurityReason.com

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

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

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

Red Hat Customer Portal

CVE-2010-0738 and JBoss Products - Red Hat Customer Portal

CVE-2010-0738 - Red Hat Customer Portal

CVE Program record

NVD vulnerability detail

CISA Known Exploited Vulnerabilities catalog

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
ADP	2022-05-25T00:00:00.000Z	CVE-2010-0738 added to CISA KEV

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](#)