

CVE-2010-1428

Red Hat JBoss Information Disclosure Vulnerability

CISA KEV since May 25, 2022

Actively exploited

Ransomware use known

Public exploit module (Metasploit)

The Web Console (aka web-console) in JBossAs in Red Hat JBoss Enterprise Application Platform (aka JBoss EAP or JBEAP) 4.2 before 4.2.0.CP09 and 4.3 before 4.3.0.CP08 performs access control only for the GET and POST methods, which allows remote attackers to obtain sensitive information via an unspecified request that uses a different method.

EVRS 80/₁₀₀ Urgent priority	CVSS V3.1 7.5 High · NVD	EPSS 0.615 99.17th percentile · FIRST	CISA DEADLINE Jun 15, 2022 KEV since 2022 · listed over a year
--	--	---	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☒ Ransomware	Known ransomware campaigns	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.615 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.5	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
jboss enterprise application platform	4.2.0 4.3.0	no fixed version listed	NVD

Sources

Vendor guidance	rhn.redhat.com/errata/RHSA-2010-0376.html	NVD	nvd.nist.gov/vuln/detail/CVE-2010-1428
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	europa.eu/enisa/eu-vulnerability/EUVD-2010-1456
Current data	evulnable.com/vulnerability-management/cve/CVE-2010-1428		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.