



# CVE-2010-1871

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2010-1871
<b>State</b>	PUBLISHED
<b>Assigner</b>	mitre
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2010-08-05 13:23:09 UTC
<b>Updated</b>	2026-04-22 14:14:18 UTC
<b>Description</b>	JBoss Seam 2 (jboss-seam2), as used in JBoss Enterprise Application Platform 4.3.0 for Red Hat Linux, does not properly

## Risk And Classification

**Primary CVSS:** v3.1 8.8 HIGH from nvd@nist.gov

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

**EPSS:** 0.936360000 probability, percentile 0.998430000 (date 2026-04-24)

**CISA KEV:** Listed on 2021-12-10; due 2022-06-10; ransomware use Unknown

**Problem Types:** CWE-917 | n/a | CWE-917 CWE-917 Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	ADP	DECLARED	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	6.8		AV:N/AC:M/Au:N/C:P/I:P/A:P

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

### CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

### CISA Known Exploited Vulnerability

<b>Vendor</b>	Red Hat
<b>Product</b>	JBoss Seam 2
<b>Name</b>	Red Hat Linux JBoss Seam 2 Remote Code Execution Vulnerability
<b>Required Action</b>	Apply updates per vendor instructions.
<b>Notes</b>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2010-1871">https://nvd.nist.gov/vuln/detail/CVE-2010-1871</a>

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Netapp	Oncommand Balance	-	All	All	All
Application	Netapp	Oncommand Insight	-	All	All	All
Application	Netapp	Oncommand Unified Manager	-	All	All	All
Operating System	Redhat	Enterprise Linux	4	All	All	All
Operating System	Redhat	Enterprise Linux	5	All	All	All

Application	Redhat	Jboss Enterprise Application Platform	4.3.0	All	All	All
-------------	--------	---------------------------------------	-------	-----	-----	-----

### Vendor Declared Affected Products

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

### References

Reference
<a href="http://archives.neohapsis.com/archives/bugtraq/2013-05/0117.html">archives.neohapsis.com/archives/bugtraq/2013-05/0117.html</a>
SecurityTracker.com Archives - JBoss Seam Input Validation Flaw in Processing JBoss Expression Language Expressions Lets Remote User
JBoss Seam Parameterized EL Expressions Remote Code Execution Vulnerability
<a href="http://www.cisa.gov/known-exploited-vulnerabilities-catalog">www.cisa.gov/known-exploited-vulnerabilities-catalog</a>
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Bug 615956 – CVE-2010-1871 JBoss Seam / Seam2: Improper sanitization of parametrized JBoss EL expressions (ACE)
Support
CVE-2010-1871 JBoss Seam Vulnerability in Multiple NetApp Products   NetApp Product Security
IBM X-Force Exchange
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	2021-12-10T00:00:00.000Z	CVE-2010-1871 added to CISA KEV

There are currently no legacy QID mappings associated with this CVE.