

# CVE-2010-1871

## Red Hat Linux JBoss Seam 2 Remote Code Execution Vulnerability

CISA KEV since Dec 10, 2021

Actively exploited

Public exploit module (Metasploit)

JBoss Seam 2 (jboss-seam2), as used in JBoss Enterprise Application Platform 4.3.0 for Red Hat Linux, does not properly sanitize inputs for JBoss Expression Language (EL) expressions, which allows remote attackers to execute arbitrary code via a crafted URL. NOTE: this is only a vulnerability when the Java Security Manager is not properly configured.

|                                                         |                                                      |                                                                   |                                                                                            |
|---------------------------------------------------------|------------------------------------------------------|-------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| <p>EVRS</p> <p><b>81</b>/100</p> <p>Urgent priority</p> | <p>CVSS V3.1</p> <p><b>8.8</b></p> <p>High · NVD</p> | <p>EPSS</p> <p><b>0.834</b></p> <p>99.68th percentile · FIRST</p> | <p>CISA DEADLINE</p> <p><b>Jun 10, 2022</b></p> <p>KEV since 2021 · listed over a year</p> |
|---------------------------------------------------------|------------------------------------------------------|-------------------------------------------------------------------|--------------------------------------------------------------------------------------------|

### Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

|                                                     |                                          |                                                                |                                            |
|-----------------------------------------------------|------------------------------------------|----------------------------------------------------------------|--------------------------------------------|
| <input checked="" type="checkbox"/> <b>CISA KEV</b> | Listed in the catalog                    | <input type="checkbox"/> <b>Vendor exploitation</b>            | Confirmed exploitation in the wild         |
| <input type="checkbox"/> <b>Ransomware</b>          | No known ransomware campaign association | <input type="checkbox"/> <b>KEV recency</b>                    | On the CISA KEV catalog for over two years |
| <input checked="" type="checkbox"/> <b>EPSS</b>     | 0.834 probability                        | <input type="checkbox"/> <b>Pre-patch disclosure</b>           | Disclosure status unavailable              |
| <input checked="" type="checkbox"/> <b>CVSS</b>     | Base score 8.8                           | <input type="checkbox"/> <b>Microsoft Exploitability Index</b> | Not a Microsoft CVE                        |

### Remediation

**Patch This Cycle** No patch reported by the connected remediation source

**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 | 4.3.0    | no fixed version listed | NVD    |
| oncommand balance                     | —        | no fixed version listed | NVD    |
| oncommand insight                     | —        | no fixed version listed | NVD    |
| oncommand unified manager             | —        | no fixed version listed | NVD    |
| enterprise linux                      | 4<br>5   | no fixed version listed | NVD    |

### Sources

|                        |                                                                                                                             |                            |                                                                                                                                         |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| <b>Vendor guidance</b> | <a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/60794">exchange.xforce.ibmcloud.com/vulnerabilities/60794</a> | <b>Additional guidance</b> | <a href="https://security.netapp.com/advisory/ntap-20161017-0001/">security.netapp.com/advisory/ntap-20161017-0001/</a>                 |
| <b>NVD</b>             | <a href="https://nvd.nist.gov/vuln/detail/CVE-2010-1871">nvd.nist.gov/vuln/detail/CVE-2010-1871</a>                         | <b>CISA KEV</b>            | <a href="https://cisa.gov/known-exploited-vulnerabilities-catalog">cisa.gov/known-exploited-vulnerabilities-catalog</a>                 |
| <b>ENISA EUVD</b>      | <a href="https://euvd.enisa.europa.eu/vulnerability/EUVD-2010-1890">euvd.enisa.europa.eu/vulnerability/EUVD-2010-1890</a>   | <b>Current data</b>        | <a href="https://evulnable.com/vulnerability-management/cve/CVE-2010-1871">evulnable.com/vulnerability-management/cve/CVE-2010-1871</a> |

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