



CVE-2011-1484

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

Summary

CVE	CVE-2011-1484
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-07-27 02:42:00 UTC
Updated	2011-10-26 02:58:00 UTC
Description	jboss-seam.jar in the JBoss Seam 2 framework 2.2.x and earlier, as distributed in Red Hat JBoss Enterprise SOA Platform

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Jboss Enterprise Application Platform	4.3.0	cp09	All	All
Application	Redhat	Jboss Enterprise Application Platform	5.1.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.3.0	cp09	All	All
Application	Redhat	Jboss Enterprise Application Platform	5.1.0	All	All	All
Application	Redhat	Jboss Enterprise Soa Platform	4.3.0	cp04	All	All
Application	Redhat	Jboss Enterprise Soa Platform	5.1.0	All	All	All
Application	Redhat	Jboss Enterprise Soa Platform	4.3.0	cp04	All	All
Application	Redhat	Jboss Enterprise Soa Platform	5.1.0	All	All	All
Application	Redhat	Jboss Seam 2 Framework	2.0.0	beta1	All	All
Application	Redhat	Jboss Seam 2 Framework	2.0.0	cr1	All	All
Application	Redhat	Jboss Seam 2 Framework	2.0.0	cr2	All	All
Application	Redhat	Jboss Seam 2 Framework	2.0.0	cr3	All	All
Application	Redhat	Jboss Seam 2 Framework	2.0.0	ga	All	All
Application	Redhat	Jboss Seam 2 Framework	2.0.1	cr1	All	All
Application	Redhat	Jboss Seam 2 Framework	2.0.1	cr2	All	All
Application	Redhat	Jboss Seam 2 Framework	2.0.1	ga	All	All
Application	Redhat	Jboss Seam 2 Framework	2.0.2	cr1	All	All

Application	Redhat	Jboss Seam 2 Framework	2.0.2	cr2	All	All
Application	Redhat	Jboss Seam 2 Framework	2.0.2	ga	All	All
Application	Redhat	Jboss Seam 2 Framework	2.0.2	sp1	All	All
Application	Redhat	Jboss Seam 2 Framework	2.0.3	cr1	All	All
Application	Redhat	Jboss Seam 2 Framework	2.1.0	alpha1	All	All
Application	Redhat	Jboss Seam 2 Framework	2.1.0	beta1	All	All
Application	Redhat	Jboss Seam 2 Framework	2.1.0	cr1	All	All
Application	Redhat	Jboss Seam 2 Framework	2.1.0	ga	All	All
Application	Redhat	Jboss Seam 2 Framework	2.1.0	sp1	All	All
Application	Redhat	Jboss Seam 2 Framework	2.1.1	cr1	All	All
Application	Redhat	Jboss Seam 2 Framework	2.1.1	cr2	All	All
Application	Redhat	Jboss Seam 2 Framework	2.1.1	ga	All	All
Application	Redhat	Jboss Seam 2 Framework	2.1.2	All	All	All
Application	Redhat	Jboss Seam 2 Framework	2.1.2	cr1	All	All
Application	Redhat	Jboss Seam 2 Framework	2.1.2	cr2	All	All
Application	Redhat	Jboss Seam 2 Framework	2.2.0	cr1	All	All
Application	Redhat	Jboss Seam 2 Framework	2.2.0	ga	All	All
Application	Redhat	Jboss Seam 2 Framework	2.2.1	All	All	All
Application	Redhat	Jboss Seam 2 Framework	2.2.1	cr1	All	All
Application	Redhat	Jboss Seam 2 Framework	2.2.1	cr2	All	All
Application	Redhat	Jboss Seam 2 Framework	2.2.1	cr3	All	All
Application	Redhat	Jboss Seam 2 Framework	2.0.0	beta1	All	All
Application	Redhat	Jboss Seam 2 Framework	2.0.0	cr1	All	All
Application	Redhat	Jboss Seam 2 Framework	2.0.0	cr2	All	All
Application	Redhat	Jboss Seam 2 Framework	2.0.0	cr3	All	All
Application	Redhat	Jboss Seam 2 Framework	2.0.0	ga	All	All
Application	Redhat	Jboss Seam 2 Framework	2.0.1	cr1	All	All
Application	Redhat	Jboss Seam 2 Framework	2.0.1	cr2	All	All
Application	Redhat	Jboss Seam 2 Framework	2.0.1	ga	All	All
Application	Redhat	Jboss Seam 2 Framework	2.0.2	cr1	All	All
Application	Redhat	Jboss Seam 2 Framework	2.0.2	cr2	All	All
Application	Redhat	Jboss Seam 2 Framework	2.0.2	ga	All	All
Application	Redhat	Jboss Seam 2 Framework	2.0.2	sp1	All	All
Application	Redhat	Jboss Seam 2 Framework	2.0.3	cr1	All	All
Application	Redhat	Jboss Seam 2 Framework	2.1.0	alpha1	All	All

Application	Redhat	Jboss Seam 2 Framework	2.1.0	beta1	All	All
Application	Redhat	Jboss Seam 2 Framework	2.1.0	cr1	All	All
Application	Redhat	Jboss Seam 2 Framework	2.1.0	ga	All	All
Application	Redhat	Jboss Seam 2 Framework	2.1.0	sp1	All	All
Application	Redhat	Jboss Seam 2 Framework	2.1.1	cr1	All	All
Application	Redhat	Jboss Seam 2 Framework	2.1.1	cr2	All	All
Application	Redhat	Jboss Seam 2 Framework	2.1.1	ga	All	All
Application	Redhat	Jboss Seam 2 Framework	2.1.2	All	All	All
Application	Redhat	Jboss Seam 2 Framework	2.1.2	cr1	All	All
Application	Redhat	Jboss Seam 2 Framework	2.1.2	cr2	All	All
Application	Redhat	Jboss Seam 2 Framework	2.2.0	cr1	All	All
Application	Redhat	Jboss Seam 2 Framework	2.2.0	ga	All	All
Application	Redhat	Jboss Seam 2 Framework	2.2.1	All	All	All
Application	Redhat	Jboss Seam 2 Framework	2.2.1	cr1	All	All
Application	Redhat	Jboss Seam 2 Framework	2.2.1	cr2	All	All
Application	Redhat	Jboss Seam 2 Framework	2.2.1	cr3	All	All
Application	Redhat	Jboss Seam 2 Framework	All	All	All	All

References

Reference	Source	Link
Support	REDHAT	www.redhat.co
Support	REDHAT	www.redhat.co
Support	REDHAT	www.redhat.co
5. Issues	CONFIRM	docs.redhat.co
Support	REDHAT	www.redhat.co
Bug 692421 – CVE-2011-1484 JBoss Seam privilege escalation caused by EL interpolation in FacesMessages	CONFIRM	bugzilla.redhat
Support	REDHAT	www.redhat.co
Support	REDHAT	www.redhat.co
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)