

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans JBoss

---

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>  
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-671>

---

### Gestion du document

Référence	CERTA-2011-AVI-671
Titre	Vulnérabilités dans JBoss
Date de la première version	05 décembre 2011
Date de la dernière version	–
Source	Bulletin de suivi de bogues JBoss AS7-2400 du 01 décembre 2011
Pièce(s) jointe(s)	Aucune

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

## 1 Risque

- Injection de code indirecte à distance ;
- injection de requêtes illégitime par rebond.

## 2 Systèmes affectés

JBoss AS 7.

## 3 Résumé

Deux vulnérabilités de JBoss permettent respectivement de l'injection de code indirecte à distance et de l'injection de requêtes illégitimes par rebond.

## 4 Description

Une vulnérabilité dans l'interface d'administration de JBoss est due à un manque de filtrage d'entrées, dont le paramètre *onerror*. Cette insuffisance est exploitable pour réaliser des injections de code indirectes à distance (XSS).

Un défaut de restriction des accès par cette même console d'administration permet à un utilisateur malveillant d'injecter des requêtes illégitimes par rebond (CSRF).

## **5 Solution**

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

## **6 Documentation**

- Bulletin de suivi de bogues JBoss AS7-2400 du 01 décembre 2011 :  
<https://issues.jboss.org/browse/AS7-2400>
- Référence CVE CVE-2011-3606 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3606>
- Référence CVE CVE-2011-3609 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3609>

## **Gestion détaillée du document**

**05 décembre 2011** version initiale.