

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de 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-2009-AVI-100>

---

### Gestion du document

Référence	CERTA-2009-AVI-100
Titre	Vulnérabilité de JBoss
Date de la première version	18 mars 2009
Date de la dernière version	–
Source(s)	Bulletins de sécurité Red Hat RHSA-2009-0346 à 0349 du 06 mars 2009
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

- Contournement de la politique de sécurité ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

- JBoss EAP 4.2, les versions antérieures à la 4.2.0.CP06 ;
- JBoss EAP 4.3, les versions antérieures à la 4.3.0.CP04.

## 3 Résumé

Un défaut du module JBossWS permettant de lire des fichiers arbitraires au format XML a été corrigé.

## 4 Description

Dans le module JBossWS, un défaut lors du traitement des requêtes d'un fichier au format WSDL permet à un attaquant de lire des fichiers arbitraires au format XML, et cela au moyen d'une requête spécialement réalisée.

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité RedHat RHSA-2009:0346 du 06 mars 2009 :  
<http://rhn.redhat.com/errata/RHSA-2009-0346.html>
- Bulletin de sécurité RedHat RHSA-2009:0347 du 06 mars 2009 :  
<http://rhn.redhat.com/errata/RHSA-2009-0347.html>
- Bulletin de sécurité RedHat RHSA-2009:0348 du 06 mars 2009 :  
<http://rhn.redhat.com/errata/RHSA-2009-0348.html>
- Bulletin de sécurité RedHat RHSA-2009:0349 du 06 mars 2009 :  
<http://rhn.redhat.com/errata/RHSA-2009-0349.html>
- Référence CVE CVE-2002-0027 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0027>

## Gestion détaillée du document

**18 mars 2009** version initiale.