

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-2007-AVI-548>

Gestion du document

Référence	CERTA-2007-AVI-548
Titre	Vulnérabilité de JBoss
Date de la première version	18 décembre 2007
Date de la dernière version	–
Source(s)	–
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

- Atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

JBoss Seam, versions 1.x.

3 Résumé

Une vulnérabilité dans JBoss Seam permet à un utilisateur malveillant de manipuler indûment des données à distance.

4 Description

Le contenu de la variable *order*, paramètre d'entrée pour la méthode *getRenderedEjbql()*, n'est pas suffisamment filtré. Cette insuffisance permet à un utilisateur malveillant d'injecter des requêtes SQL. Ce dernier peut alors porter atteinte à la confidentialité ou à l'intégrité des données de la base.

5 Solution

La version 2.0.0.GA résoud le problème. Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de changement de JBoss Seam :
http://sourceforge.net/project/shownotes.php?release_id=549490&group_id=22866
- Bulletin JBSEAM-2084 du 14 octobre 2007 :
<http://jira.jboss.com/jira/browse/JBSEAM-2084>

Gestion détaillée du document

18 décembre 2007 version initiale.