Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 16 décembre 2011
N° CERTA-2011-AVI-703

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans JBoss

Gestion du document

Référence	CERTA-2011-AVI-703
Titre	Vulnérabilités dans JBoss
Date de la première version	16 décembre 2011
Date de la dernière version	–
Source	Bulletin de sécurité RedHat RHSA-2011:1822 du 14 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

- Contournement de la politique de sécurité ;
- injection de code indirecte à distance.

2 Systèmes affectés

JBoss Enterprise Portal Platform, versions antérieures à la version 5.2.0.

3 Résumé

Plusieurs vulnérabilités affectent JBoss. Elles permettent de contourner la politique de sécurité du serveur ou de réaliser de l'injection de code indirecte (XSS).

4 Description

Plusieurs vulnérabilités affectent JBoss :

- la page de connexion au serveur permet de rediriger l'utilisateur vers un site web quelconque ;
- dans certaines configurations, l'authentification de l'utilisateur peut être contournée ;

– de l'injection de code indirecte est possible dans plusieurs programmes de JBoss.

5 Solution

La version 5.2.0 de JBoss corrige ces vulnérabilités.
Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

– Bulletin de sécurité RedHat RHSA-2011:1822 du 14 décembre 2011 :
http://rhn.redhat.com/errata/RHSA-2011-1822.html
– Référence CVE CVE-2011-2941 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2941
– Référence CVE CVE-2011-4085 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-4085
– Référence CVE CVE-2011-4580 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-4580

Gestion détaillée du document

16 décembre 2011 version initiale.