



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 08 février 2012
N° CERTA-2012-AVI-066

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans JBoss Enterprise Platform

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-2012-AVI-066>

Gestion du document

Référence	CERTA-2012-AVI-066
Titre	Vulnérabilité dans JBoss Enterprise Platform
Date de la première version	08 février 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité Red Hat RHSA-2012-0091
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

- Exécution de code arbitraire à distance ;
- déni de service à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

JBoss Enterprise Portal Platform 4.x.

3 Résumé

Plusieurs vulnérabilités permettant de contourner la politique de sécurité, d'exécuter du code arbitraire ou de réaliser un déni de service à distance ont été corrigées dans JBoss Enterprise Portal Platform.

4 Description

De multiples vulnérabilités ont été corrigées dans JBoss Enterprise Portal Platform. Ces vulnérabilités peuvent être exploitées pour :

- exécuter du code Java arbitraire à distance (CVE-2011-1484) ;

- provoquer un déni de service à distance (CVE-2011-4858) ;
- effectuer des rejeux de session (CVE-2011-1184, CVE-2011-5062, CVE-2011-5063, CVE-2011-5064) ;
- effectuer des requêtes non authentifiées (CVE-2011-4085) ;
- contourner les restrictions d'accès à certains fichiers (CVE-2011-2526).

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-2012:0091 du 02 février 2012 :
<http://rhn.redhat.com/errata/RHSA-2012-0091.html>
- Référence CVE-2011-1184 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1184>
- Référence CVE-2011-1484 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1484>
- Référence CVE-2011-2526 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2526>
- Référence CVE-2011-4085 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-4085>
- Référence CVE-2011-4858 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-4858>
- Référence CVE-2011-5062 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-5062>
- Référence CVE-2011-5063 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-5063>
- Référence CVE-2011-5064 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-5064>

Gestion détaillée du document

08 février 2012 version initiale.