

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité 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-2012-AVI-042>

Gestion du document

Référence	CERTA-2012-AVI-042
Titre	Vulnérabilité dans JBoss
Date de la première version	31 janvier 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité redhat RHSA-2012:0035 Bulletin de sécurité redhat RHSA-2012:0036 Bulletin de sécurité redhat RHSA-2012:0037 Bulletin de sécurité redhat RHSA-2012:0038 Bulletin de sécurité redhat RHSA-2012:0039 Bulletin de sécurité redhat RHSA-2012:0040
Pièce(s) jointe(s)	Aucune

TAB. 1 – Gestion du document

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

1 Risques

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

2 Systèmes affectés

- JBoss Enterprise Web Server 1.0 for RHEL 4 AS ;
- JBoss Enterprise Web Server 1.0 for RHEL 5 Server ;
- JBoss Enterprise Web Server 1.0 for RHEL 6 Server ;
- JBoss Enterprise Web Server 1.0 ;
- JBoss Enterprise Application Platform 5 for RHEL 4 AS (mod_cluster-native) ;
- JBoss Enterprise Application Platform 5 for RHEL 5 AS (mod_cluster-native) ;
- JBoss Enterprise Application Platform 5 for RHEL 6 AS (mod_cluster-native) ;

- JBoss Enterprise Application Platform 5.1 ;
- JBoss Enterprise Web Platform 5 for RHEL 4 AS (mod_cluster-native) ;
- JBoss Enterprise Web Platform 5 for RHEL 5 Server (mod_cluster-native) ;
- JBoss Enterprise Web Platform 5 for RHEL 6 Server (mod_cluster-native) ;
- JBoss Enterprise Web Platform 5.1.

3 Résumé

Une vulnérabilité dans le module *mod_cluster* de *JBoss Enterprise Application Platform* pour *Red Hat Linux* permet à un utilisateur malintentionné distant de contourner la politique de sécurité, voler des identifiants de session et d'élever ses privilèges.

4 Description

Le module *mod_cluster* de *JBoss Enterprise Application Platform* pour *Red Hat Linux* autorise les noeuds de travail à s'enregistrer auprès de n'importe quel hôte virtuel. Une personne malintentionnée peut alors forcer un enregistrement auprès d'un hôte virtuel externe qui ne met en place aucune restriction de sécurité et, ainsi, passer outre la politique de sécurité. L'attaquant peut alors voler des données sensibles comme des informations d'identification, afin d'élever ses privilèges, ou bien encore proposer du contenu malveillant à des utilisateurs légitimes.

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-2012:0035 du 18 janvier 2012 :
<http://rhn.redhat.com/errata/RHSA-2012-0035.html>
- Bulletin de sécurité RedHat RHSA-2012:0036 du 18 janvier 2012 :
<http://rhn.redhat.com/errata/RHSA-2012-0036.html>
- Bulletin de sécurité RedHat RHSA-2012:0037 du 18 janvier 2012 :
<http://rhn.redhat.com/errata/RHSA-2012-0037.html>
- Bulletin de sécurité RedHat RHSA-2012:0038 du 18 janvier 2012 :
<http://rhn.redhat.com/errata/RHSA-2012-0038.html>
- Bulletin de sécurité RedHat RHSA-2012:0039 du 18 janvier 2012 :
<http://rhn.redhat.com/errata/RHSA-2012-0039.html>
- Bulletin de sécurité RedHat RHSA-2012:0040 du 18 janvier 2012 :
<http://rhn.redhat.com/errata/RHSA-2012-0040.html>
- Référence CVE CVE-2011-4608 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-4608>

Gestion détaillée du document

31 janvier 2012 version initiale.