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-065

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans JBoss Operations Network

Gestion du document

Référence	CERTA-2012-AVI-065
Titre	Multiples vulnérabilités dans JBoss Operations Network
Date de la première version	08 février 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité REDHAT RHSA-2012:0089-1 du 01 février 2012
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.

2 Systèmes affectés

JBoss Operations Network versions 2.4.1 et inférieures.

3 Résumé

De multiples vulnérabilités ont été corrigées dans *JBoss Operations Network*.

4 Description

Une mise à jour de *JBoss Operations Network* corrige de multiples vulnérabilités. Les vulnérabilités associées à un numéro CVE sont les suivantes :

– CVE-2012-0052 et CVE-2012-0062 : ces vulnérabilités permettent à un utilisateur distant malintentionné de détourner la session d'un agent approuvé et de voler son jeton de sécurité. Ceci permettra à l'attaquant de récupérer des informations sensibles à propos du serveur sur lequel l'agent s'exécute ;

- CVE-2011-4858 : cette vulnérabilité permet à un attaquant d'effectuer un déni de service à distance sur le serveur *JBoss Web* ;
- CVE-2011-3206 : cette vulnérabilité concerne de multiples failles XSS dans l'interface d'administration de *JBoss Operations Network* ;
- CVE-2011-4573 : cette vulnérabilité concerne une vérification qui n'est pas effectuée correctement par *JBoss Operations Network* lorsqu'un utilisateur tente de supprimer une mise à jour de configuration de *plugin* (*plug-in configuration update*).

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-2012:0089 du 08 février 2012 :
  http://rhn.redhat.com/errata/RHSA-2012-0089.html
- Référence CVE CVE-2011-3206 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3206
- Référence CVE CVE-2011-4573 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-4573
- Référence CVE CVE-2011-4858 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-4858
- Référence CVE CVE-2012-0052 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0052
- Référence CVE CVE-2012-0062 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0062

Gestion détaillée du document

08 février 2012 version initiale.