



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 septembre 2011
N° CERTA-2011-AVI-515

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans IBM WebSphere

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-2011-AVI-515>

Gestion du document

Référence	CERTA-2011-AVI-515
Titre	Vulnérabilités dans IBM WebSphere
Date de la première version	14 septembre 2011
Date de la dernière version	–
Source	Bulletin de sécurité IBM swg27014463 du 12 septembre 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

- Dénis de service à distance ;
- atteinte à la confidentialité des données ;
- contournement de la politique de sécurité ;
- injection de requêtes illégitime par rebond.

2 Systèmes affectés

IBM WebSphere 6.x et 7.x.

3 Résumé

Plusieurs vulnérabilités ont été corrigées dans IBM WebSphere. Elles permettent diverses atteintes à la disponibilité, à l'intégrité et à la confidentialité.

4 Description

Plusieurs vulnérabilités ont été corrigées dans IBM WebSphere :

- lors de la déconnexion d'un utilisateur, celui-ci peut être dérouté vers une page non légitime, permettant par exemple le filoutage ;
- un problème dans la bibliothèque de programmes APR (*Apache Portable Runtime*) permet à un utilisateur malveillant d'épuiser les ressources processeur à distance ;
- un utilisateur local peut obtenir des informations sensibles au moyen d'une requête spécialement construite à destination de la console d'administration ;
- la vérification de validité des certificats de clefs publiques est incorrecte ;
- la console d'administration permet l'injection de requêtes par rebond (CRSF) ;
- un utilisateur distant peut, sans autorisation, parcourir l'arborescence du système de fichiers au moyen d'une adresse (URI) particulière ;
- l'encapsulation de signatures XML permet de contourner l'authentification.

5 Solution

Les versions IBM WebSphere 6.1.0.39 et 7.0.0.19 résolvent ces problèmes.

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité IBM swg27014463 du 12 septembre 2011 :
<http://www-01.ibm.com/support/docview.wss?uid=swg27014463#70019>
- Bulletin de sécurité IBM swg27007951 du 18 juillet 2011 :
<http://www-01.ibm.com/support/docview.wss?uid=swg27007951#61039>
- Référence CVE CVE-2011-0419 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0419>
- Référence CVE CVE-2011-1355 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1355>
- Référence CVE CVE-2011-1356 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1356>
- Référence CVE CVE-2011-1359 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1359>
- Référence CVE CVE-2011-1411 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1411>

Gestion détaillée du document

14 septembre 2011 version initiale.