Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 30 mars 2010
N° CERTA-2010-AVI-142

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans IBM WebSphere

Gestion du document

Référence	CERTA-2010-AVI-142
Titre	Vulnérabilités dans IBM WebSphere
Date de la première version	30 mars 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité IBM swg27004980 du 29 mars 2010
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

- Déni de service à distance ;
- atteinte à la confidentialité des données ;
- injection de code indirecte à distance.

2 Systèmes affectés

IBM WebSphere 7.0.x, 6.1.x et 6.0.x.

3 Résumé

Plusieurs vulnérabilités présentes dans IBM WebSphere permettent à un utilisateur malveillant d'accéder à des données, de provoquer un déni de service à distance ou de réaliser de l'injection de code indirecte.

4 Description

Plusieurs vulnérabilités affectant IBM WebSphere ont été publiées :

- (CVE-2010-0768) dans la console d'administration, un manque de vérification des données entrées est exploitable par un utilisateur malveillant pour réaliser de l'injection de code indirecte ;

– (CVE-2010-0769) un défaut dans WebSphere Application Server permet à un utilisateur distant authentifié de lire des mots de passe non chiffrés ;
– (CVE-2010-0770) une erreur dans le traitement des sessions SSL avec un client ORB (*Object Request Broker*) permet à un utilisateur distant authentifié de provoquer un déni de service par attente infinie du serveur.

5 Solution

Les versions 6.0.2.41, 6.1.0.31 et 7.0.0.9 d'IBM WebSphere remédient à ces vulnérabilités. Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

– Bulletin de sécurité IBM swg27004980 du 29 mars 2010 :
http://www-01.ibm.com/support/docview.wss?uid=swg27004980
– Référence CVE CVE-2010-0768 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0768
– Référence CVE CVE-2010-0769 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0769
– Référence CVE CVE-2010-0770 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0770

Gestion détaillée du document

30 mars 2010 version initiale.