



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 04 décembre 2009  
N° CERTA-2009-AVI-529

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-2009-AVI-529>

---

### Gestion du document

Référence	CERTA-2009-AVI-529
Titre	Vulnérabilités dans IBM WebSphere
Date de la première version	04 décembre 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité IBM swg1PK96157 du 02 décembre 2009
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 ;
- contournement de la politique de sécurité.

## 2 Systèmes affectés

*IBM WebSphere*, versions 6.0.x sur systèmes z/OS.

## 3 Résumé

Plusieurs vulnérabilités présentes dans *IBM WebSphere* ont été corrigées. Ces vulnérabilités permettent de provoquer un déni de service à distance ou de contourner la politique de sécurité.

## 4 Description

Plusieurs vulnérabilités, de type dépassement d'entier, ont été découvertes dans les outils de la librairie d'exécution *Apache Portable Runtime* (APR-Utility) utilisée par *IBM WebSphere*. Ces vulnérabilités permettent à une personne distante malintentionnée d'exécuter du code arbitraire.

De nombreuses vulnérabilités ont été découvertes dans le serveur HTTP. L'exploitation de ces vulnérabilités permet d'accéder à des informations sensibles ou de réaliser un déni de service à distance.

Deux vulnérabilités concernent le module `mod_proxy_ftp`. La première est de type pointeur nul et permet de provoquer un déni de service par le biais d'un serveur FTP construit de manière particulière. La seconde permet à un attaquant d'envoyer des commandes FTP arbitraires en utilisant le serveur Apache en tant que serveur mandataire.

Une vulnérabilité a été identifiée dans les protocoles SSL et TLS lors de renégociations de sessions. Un utilisateur s'étant au préalable intercalé dans la transmission (*man in the middle*) peut, dans certaines circonstances, injecter des données au détriment d'un utilisateur légitime, pour, par exemple, forcer l'envoi d'une requête HTTP au serveur vers lequel la victime se connecte.

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité IBM swg1PK96157 du 02 décembre 2009 :  
<http://www-01.ibm.com/support/docview.wss?uid=swg1PK96157>
- Document du CERTA CERTA-2009-AVI-323 du 20 octobre 2009 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-323/index.html>
- Document du CERTA CERTA-2009-AVI-408 du 25 septembre 2009 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-408/index.html>
- Document du CERTA CERTA-2009-AVI-424 du 07 octobre 2009 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-424/index.html>
- Document du CERTA CERTA-2009-AVI-482 du 27 novembre 2009 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-482/index.html>
- Bulletin de sécurité IBM swg1PK96157 du 02 décembre 2009 :  
<http://www-01.ibm.com/support/docview.wss?uid=swg1PK96157>
- Référence CVE CVE-2009-1891 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1891>
- Référence CVE CVE-2009-2412 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2412>
- Référence CVE CVE-2009-3094 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3094>
- Référence CVE CVE-2009-3555 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3555>

## Gestion détaillée du document

**04 décembre 2009** version initiale.