

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans IBM WebSphere Application Server

---

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-341>

---

### Gestion du document

Référence	CERTA-2009-AVI-341
Titre	Vulnérabilités dans IBM WebSphere Application Server
Date de la première version	18 août 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité IBM swg27014463 du 27 juillet 2009 et swg27007951 du 05 août 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 ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

IBM WebSphere Application Server 6.x et 7.x.

## 3 Résumé

Plusieurs vulnérabilités dans IBM WebSphere Application Server ont été publiées. Certaines permettent à un utilisateur malveillant d'exécuter du code arbitraire à distance.

## 4 Description

Plusieurs vulnérabilités dans IBM WebSphere Application Server ont été publiées :

- le composant *Security* présente un défaut qui permet à un utilisateur malveillant de contourner à distance les restrictions d'accès ;
- un problème dans le composant *Web Service* permet à un utilisateur local de réaliser un déni de service ;
- dans certaines configurations, lors de l'utilisation de *SPNEGO Single Sign-On*, un utilisateur malveillant distant peut contourner l'authentification ;
- le composant de migration permet à un utilisateur authentifié distant d'obtenir indûment des informations sensibles ;
- un défaut non précisé du composant *System Management/Repository* permet à un utilisateur malveillant distant de contourner les restrictions d'accès et d'arrêter un service ;
- sur un système *z/OS*, le composant *System Management/Repository* utilise des droits d'accès permissifs, permettant à un utilisateur malveillant d'obtenir des données sensibles ;
- une lecture erronée du paramètre *portletServingEnabled* permet à un utilisateur malveillant distant de contourner les restrictions d'accès.

## 5 Solution

Les versions 7.0.0.5 et 6.1.0.25 corrigent 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 swg27014463 du 27 juillet 2009 :  
<http://www-01.ibm.com/support/docview.wss?uid=swg27014463>
- Bulletin de sécurité IBM swg27007951 du 05 août 2009 :  
<http://www-01.ibm.com/support/docview.wss?uid=swg27007951>
- Référence CVE CVE-2009-2085 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2085>
- Référence CVE CVE-2009-2087 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2087>
- Référence CVE CVE-2009-2088 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2088>
- Référence CVE CVE-2009-2089 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2089>
- Référence CVE CVE-2009-2090 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2090>
- Référence CVE CVE-2009-2091 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2091>
- Référence CVE CVE-2009-2092 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2092>

## Gestion détaillée du document

18 août 2009 version initiale.