

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples 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-2006-AVI-451>

---

### Gestion du document

Référence	CERTA-2006-AVI-451
Titre	Multiples vulnérabilités dans IBM Websphere
Date de la première version	12 octobre 2006
Date de la dernière version	–
Source(s)	Bulletin de mise à jour IBM Websphere
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 ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

IBM WebSphere Application Server 6.1.x

## 3 Résumé

De multiples vulnérabilités ont été découvertes dans IBM Websphere. L'exploitation de ces vulnérabilités conduit au contournement de la politique de sécurité et/ou à la divulgation d'informations sensibles.

## 4 Description

Trois vulnérabilités ont été découvertes dans IBM Websphere Application Server :

- la première découle d'une erreur présente au niveau du traitement de certaines requêtes HTTP. L'exploitation de cette vulnérabilité conduit à l'accès au code source d'une page JSP ;

- la deuxième découle d'une erreur inconnue dans WSN. Un utilisateur mal intentionné peut exploiter cette vulnérabilité afin d'obtenir un accès à la machine vulnérable sans fournir d'identifiant ;
- la troisième permet à un utilisateur mal intentionné d'accéder de manière illégitime à des données.

## **5 Solution**

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

## **6 Documentation**

- Bulletin de mise à jour IBM Websphere :  
<http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg24013142>
- Référence CVE CVE-2006-4223 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4223>

## **Gestion détaillée du document**

**12 octobre 2006** version initiale.