



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 17 mai 2006  
N° CERTA-2006-AVI-203

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités de BEA WebLogic

---

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-203>

---

### Gestion du document

|                             |  |
|-----------------------------|--|
| Référence                   | CERTA-2006-AVI-203                               |
| Titre                       | Multiples vulnérabilités de BEA WebLogic         |
| Date de la première version | 17 mai 2006                                      |
| Date de la dernière version | –  |
| Source(s)                   | Bulletin de sécurité du vendeur BEA Systems Inc. |
| 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

- BEA WebLogic Server 6.X ;
- BEA WebLogic Server 7.X ;
- BEA WebLogic Server 8.X ;
- BEA WebLogic Server 9.X ;
- BEA WebLogic Express 6.X ;
- BEA WebLogic Express 7.X ;
- BEA WebLogic Express 8.X ;
- BEA WebLogic Express 9.X.

### 3 Résumé

Plusieurs vulnérabilités ont été identifiées dans certaines versions de WebLogic Server et WebLogic Express fournies par BEA Systems Inc. Elles permettent à un utilisateur malveillant de contourner la politique de sécurité par différentes manières.

### 4 Description

BEA WebLogic Server et WebLogic Express sont des serveurs d'application aidant à la création et au développement des services Web. Plusieurs vulnérabilités impliquant la majorité des versions actuelles ont été identifiées. Elles permettent à un utilisateur malveillant de contourner des politiques de sécurité. Parmi celles-ci :

- Des données sensibles peuvent être interceptées au cours d'échanges JTA (pour *Java Transaction API*) dans des canaux non-sécurisés.
- Un client exigeant un canal d'échange sécurisé peut ne pas l'obtenir du fait d'une mauvaise configuration de la *Quality of Service*.
- Sous certaines conditions, le mot de passe administrateur est écrit en clair dans des fichiers système du serveur.
- Une mauvaise compilation de code JSP (JavaServer Pages) permet dans certains cas d'accéder au code source à distance.
- L'adresse IP propre du serveur est visible dans la console d'administration de certaines versions.
- Si l'accès à distance par HTTP à une application web ou un JWS protégé (pour *Java Web Start*) échoue, le nom d'accès et le mot de passe sont écrits dans les journaux du serveur.
- L'accès à des clefs privées du serveur n'est pas restreint. Les clefs sont donc accessibles par des applications tierces installées sur la même machine que le serveur.
- La commande `stopWebLogic.sh` du serveur peut entraîner l'affichage du mot de passe administrateur en clair dans la sortie standard `stdout`.

### 5 Solution

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

### 6 Documentation

- Bulletin de sécurité BEA06-133-00 de BEA Systems : <http://dev2dev.bea.com/pub/advisory/195>
- Bulletin de sécurité BEA06-132-00 de BEA Systems : <http://dev2dev.bea.com/pub/advisory/194>
- Bulletin de sécurité BEA06-131-00 de BEA Systems : <http://dev2dev.bea.com/pub/advisory/193>
- Bulletin de sécurité BEA06-130-00 de BEA Systems : <http://dev2dev.bea.com/pub/advisory/192>
- Bulletin de sécurité BEA06-129-00 de BEA Systems : <http://dev2dev.bea.com/pub/advisory/191>
- Bulletin de sécurité BEA06-128-00 de BEA Systems : <http://dev2dev.bea.com/pub/advisory/190>
- Bulletin de sécurité BEA06-127-00 de BEA Systems : <http://dev2dev.bea.com/pub/advisory/189>
- Bulletin de sécurité BEA06-126-00 de BEA Systems : <http://dev2dev.bea.com/pub/advisory/188>
- Bulletin de sécurité BEA06-125-00 de BEA Systems : <http://dev2dev.bea.com/pub/advisory/187>
- Bulletin de sécurité BEA06-124-00 de BEA Systems : <http://dev2dev.bea.com/pub/advisory/186>
- Bulletin de sécurité BEA06-121-00 de BEA Systems : <http://dev2dev.bea.com/pub/advisory/181>

# **Gestion détaillée du document**

**17 mai 2006** version initiale.