

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Failles multiples des serveurs WebLogic de BEA

---

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-2004-AVI-142>

---

### Gestion du document

Référence	CERTA-2004-AVI-142
Titre	Failles multiples des serveurs WebLogic de BEA
Date de la première version	26 avril 2004
Date de la dernière version	–
Source(s)	Avis de sécurité de BEA
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

- Usurpation de privilèges ;
- divulgation d'informations ;
- déni de service.

## 2 Systèmes affectés

Quelle que soit le système d'exploitation :

- *WebLogic Server* et *Express 8.1* jusqu'au *Service Pack 2* ;
- *WebLogic Server* et *Express 7.0* jusqu'au *Service Pack 4* ;
- *WebLogic Server* et *Express 6.1* jusqu'au *Service pack 6*.

## 3 Résumé

Sept vulnérabilités différentes ont été publiées par *BEA* :

1. il est possible d'obtenir l'identifiant et l'authentifiant de l'administrateur ;

2. il est possible, dans certains cas, de dérober l'identifiant et l'authentifiant de l'utilisateur ayant lancé le serveur ;
3. un certificat X509 habilement construit peut permettre d'usurper l'identité d'un utilisateur légitime lors d'une connexion SSL ;
4. certains objets EJB ("*Enterprise Java Beans*") peuvent être retirés par des utilisateurs n'en ayant pas les droits ;
5. l'identifiant et l'authentifiant d'accès à la base de données sont stockés en clair ;
6. les privilèges d'un groupe supprimé peuvent être indûment accordés à ses membres lors de sa re-crédation ;
7. une faiblesse peut être utilisée pour contourner une restriction sur les adresses réticulaires (*URL*) accessibles.

## 4 Description

Les serveurs *WebLogic* de la société *BEA*, fournissent un support pour le déploiement d'applications Java distribuées (serveur *J2EE*). Les failles recensées sont les suivantes :

1. l'accès au journaux de l'assistant de configuration ("*assistant wizard*") permet d'obtenir l'identifiant et l'authentifiant de l'administrateur (version 8.1) ;
2. un utilisateur ayant des privilèges pour installer et exécuter du code peut dérober l'identifiant et le mot de passe du compte ayant démarré le serveur (versions 8.1 et 7.0) ;
3. les sites utilisant un gestionnaire de confiance personnalisé ("*custom trust manager*") pour les certificats X509 risquent qu'un certificat refusé par le gestionnaire soit tout de même accepté par le serveur (versions 8.1 et 7.0) ;
4. une application EJB possédant une méthode *remove()*, peut voir cette dernière activée par des utilisateurs n'en ayant normalement pas le privilège (version 8.1, 7.0 et 6.1) ;
5. dans certains cas, l'utilisateur et le mot de passe d'accès à une base de données sont écrits en clair dans un fichier *config.xml* (versions 8.1, 7.0 et 6.1) ;
6. la re-crédation d'un groupe auparavant supprimé maintient les privilèges initiaux si des membres de la première version existent toujours (versions 8.1 et 7.0) ;
7. un mauvais format dans la spécification d'une adresse réticulaire au sein d'une application permet à un utilisateur mal intentionné de contourner les restrictions d'accès (versions 8.1 et 7.0).

## 5 Solution

Mettre à jour en suivant les recommandations du distributeur :

1. usurpation des privilèges administrateur :  
[http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04\\_58.00.jsp](http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04_58.00.jsp)
2. usurpation du compte de démarrage :  
[http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04\\_55.00.jsp](http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04_55.00.jsp)
3. mauvaise validation SSL :  
[http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04\\_54.00.jsp](http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04_54.00.jsp)
4. suppression d'objets EJB :  
[http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04\\_57.00.jsp](http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04_57.00.jsp)
5. risque d'accès à la base de donnée :  
[http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04\\_53.00.jsp](http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04_53.00.jsp)
6. conservation de privilèges :  
[http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04\\_52.01.jsp](http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04_52.01.jsp)
7. contournement des restrictions d'accès :  
[http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04\\_56.00.jsp](http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04_56.00.jsp)

## 6 Documentation

Notes de vulnérabilité de l'US-CERT :

1. usurpation des privilèges administrateur :  
<http://www.kb.cert.org/vuls/id/574222>

2. usurpation du compte de démarrage :  
<http://www.kb.cert.org/vuls/id/352110>
3. mauvaise validation SSL :  
<http://www.kb.cert.org/vuls/id/566390>
4. suppression d'objets EJB :  
<http://www.kb.cert.org/vuls/id/658878>
5. risque d'accès à la base de donnée :  
<http://www.kb.cert.org/vuls/id/920238>
6. conservation de privilèges :  
<http://www.kb.cert.org/vuls/id/470470>

## **Gestion détaillée du document**

**26 avril 2004** version initiale.