



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 juin 2004
N° CERTA-2004-AVI-201

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité 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-2004-AVI-201>

Gestion du document

| | |
|-----------------------------|----------------------------------|
| Référence | CERTA-2004-AVI-201 |
| Titre | Vulnérabilité de BEA WebLogic |
| Date de la première version | 16 juin 2004 |
| Date de la dernière version | – |
| Source(s) | Bulletin de sécurité BEA04-62.00 |
| 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

Elévation de privilèges.

2 Systèmes affectés

- BEA WebLogic Server et WebLogic Express version 8.1 ;
- BEA WebLogic Server et WebLogic Express version 7.0 ;
- BEA WebLogic Server et WebLogic Express version 6.1.

3 Résumé

Une vulnérabilité de BEA WebLogic Server et WebLogic Express permet à un utilisateur distant mal intentionné d'exécuter certaines actions sous une fausse identité.

4 Description

Il est possible pour un client de se connecter plusieurs fois à un serveur WebLogic avec différentes identités.

Lorsque ces connexions utilisent les requêtes RMI (*Remote Method Invocation*) sur le protocole IIOP (*Internet Inter-ORB Protocol*), certaines méthodes RMI de l'une des identités peuvent être exécutées avec les privilèges d'une autre identité.

5 Solution

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

6 Documentation

Bulletin de sécurité de BEA #BEA04-62.00 :

http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04_62.00.jsp

Gestion détaillée du document

16 juin 2004 version initiale.