



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 mai 2004
N° CERTA-2004-AVI-162

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans 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-162>

Gestion du document

Référence	CERTA-2004-AVI-162
Titre	Multiples vulnérabilités dans BEA WebLogic
Date de la première version	13 mai 2004
Date de la dernière version	–
Source(s)	Bulletins de sécurité 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

- Déni de service ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- WebLogic Server et WebLogic Express version 8.1 jusqu'au Service Pack 2 ;
- WebLogic Server et WebLogic Express version 7.0 jusqu'au Service Pack 5.

Toutes les plates-formes sont affectées.

3 Résumé

Deux vulnérabilités dans BEA WebLogic Server et Express permettent à un utilisateur mal intentionné de désactiver la sécurité mise en place sur une application Web ou bien d'effectuer un déni de service.

4 Description

Les serveurs WebLogic de la société BEA, fournissent un support pour le déploiement d'applications Java distribuées (serveur J2EE).

Deux vulnérabilités sont présentes dans BEA WebLogic Server et Express :

- une mauvaise gestion des "tags" lors de la mise à jour des pages WebLogic au format XML permet à un utilisateur mal intentionné d'élever ses privilèges ;
- une mauvaise gestion de la politique de sécurité permet à un utilisateur préalablement authentifié de démarrer ou de stopper le serveur sans en posséder les droits.

5 Solution

Appliquer les correctifs disponibles sur le site de l'éditeur (cf. Documentation).

6 Documentation

- Bulletin de sécurité #BEA04-59.00 de BEA :
http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04_59.00.jsp
- Bulletin de sécurité #BEA04-60.00 de BEA :
http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04_60.00.jsp

Gestion détaillée du document

13 mai 2004 version initiale.