



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 21 février 2008  
N° CERTA-2008-AVI-099

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : 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-2008-AVI-099>

---

### Gestion du document

Référence	CERTA-2008-AVI-099
Titre	Vulnérabilités de BEA Weblogic
Date de la première version	21 février 2008
Date de la dernière version	–
Source(s)	Bulletins de sécurité BEA 256 à 275
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

- Exécution de code arbitraire à distance ;
- atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

- *BEA Weblogic Express*, versions 6.x à 10.x ;
- *BEA Weblogic Portal*, versions 8.x à 10.x ;
- *BEA Weblogic Server*, versions 6.x à 10.x ;
- *BEA Weblogic Workshop*, versions 8 ;
- *BEA Workshop for Weblogic* , versions 9.x et 10.x.

## 3 Résumé

De nombreuses vulnérabilités affectent les produits *BEA Weblogic*. Leur exploitation permet à un utilisateur malveillant d'exécuter du code arbitraire à distance ou de porter atteinte à l'intégrité ou à la confidentialité des données.

## 4 Description

De nombreuses vulnérabilités affectent les produits *BEA Weblogic* :

- une erreur de traitement des requêtes par *HttpProxyServlet* et *HttpClusterServlet* permet à un utilisateur d’obtenir des droits d’administration sur le serveur, dans certaines conditions ;
- des erreurs non précisées permettent de réaliser de l’injection de code indirecte (*cross site scripting*) sur le poste de l’utilisateur ;
- une erreur dans la console d’administration permet de réaliser de l’injection de code indirecte (*cross site scripting*) sur le poste d’un administrateur ;
- des erreurs non précisées permettent de contourner la politique de sécurité, en particulier d’accéder à des servletes non autorisées ;
- un problème de gestion des sessions permet de détourner la session d’un utilisateur ;
- une erreur dans la gestion des sessions HTTPS peut conduire à une redirection en HTTP ;
- un défaut de verrouillage des comptes permet à un utilisateur malveillant de procéder à une recherche exhaustive de mots de passe ;
- la protection des mots de passe de bases de données est insuffisante. L’exploitation de cette faiblesse n’est possible que si *RDBMS Authentication* est utilisé.

## 5 Solution

Se référer aux bulletins de sécurité de l’éditeur pour l’obtention des correctifs (cf. section Documentation).

## 6 Documentation

- Bulletin de sécurité BEA 256 à 275 :  
<http://dev2dev.bea.com/pub/advisory/256>  
<http://dev2dev.bea.com/pub/advisory/257>  
<http://dev2dev.bea.com/pub/advisory/258>  
<http://dev2dev.bea.com/pub/advisory/261>  
<http://dev2dev.bea.com/pub/advisory/262>  
<http://dev2dev.bea.com/pub/advisory/263>  
<http://dev2dev.bea.com/pub/advisory/264>  
<http://dev2dev.bea.com/pub/advisory/265>  
<http://dev2dev.bea.com/pub/advisory/266>  
<http://dev2dev.bea.com/pub/advisory/267>  
<http://dev2dev.bea.com/pub/advisory/268>  
<http://dev2dev.bea.com/pub/advisory/269>  
<http://dev2dev.bea.com/pub/advisory/270>  
<http://dev2dev.bea.com/pub/advisory/271>  
<http://dev2dev.bea.com/pub/advisory/273>  
<http://dev2dev.bea.com/pub/advisory/274>  
<http://dev2dev.bea.com/pub/advisory/275>

## Gestion détaillée du document

21 février 2008 version initiale.