Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 30 août 2007
N° CERTA-2007-AVI-385

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de BEA Weblogic

Gestion du document

Référence	CERTA-2007-AVI-385
Titre	Multiples vulnérabilités de BEA Weblogic
Date de la première version	30 août 2007
Date de la dernière version	–
Source(s)	Bulletins 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

- Déni de service à distance ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- *BEA Weblogic Server*, versions 6.x, 7.x, 8.x, 9.x et 10.x ;
- *BEA Weblogic Express*, versions 6.x, 7.x, 8.x et 9.x.

3 Résumé

Plusieurs vulnérabilités affectent les produits *BEA Weblogic* et permettent à un utilisateur malveillant d'accéder à des données sensibles ou de provoquer un déni de service à distance.

4 Description

Le logiciel *BEA Weblogic* est un serveur d'applications Java (J2EE).

Plusieurs vulnérabilités affectent les produits *BEA Weblogic* :

- deux vulnérabilités dans la négociation des algorithmes de chiffrement utilisés pour une session SSL peuvent provoquer l'utilisation de l'algorithme `null`. Les données sont alors transmises en clair et accessibles à un utilisateur malveillant ;
- des requêtes particulières permettent à un utilisateur malveillant de bloquer les fils (*threads*) du serveur, donc de provoquer un déni de service à distance ;
- des requêtes avec des en-têtes malformés permettent à un utilisateur malveillant d'épuiser les ressources disque du serveur, donc de provoquer un déni de service à distance.

5 Solution

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

6 Documentation

- Bulletins de sécurité de *BEA* :
  http://dev2dev.bea.com/pub/advisory/244
  http://dev2dev.bea.com/pub/advisory/245
  http://dev2dev.bea.com/pub/advisory/246
  http://dev2dev.bea.com/pub/advisory/247

Gestion détaillée du document

30 août 2007 version initiale.