Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 23 janvier 2007
N° CERTA-2007-AVI-044

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de BEA WebLogic

Gestion du document

Référence	CERTA-2007-AVI-044
Titre	Multiples vulnérabilités de BEA WebLogic
Date de la première version	23 janvier 2007
Date de la dernière version	–
Source(s)	Avis de sécurité BEA du 16 janvier 2007
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 ;
- contournement de la politique de sécurité ;
- atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- BEA WebLogic Server et WebLogic Express version 8.1, ayant une mise à jour antérieure au Service Pack 5 ;
- BEA WebLogic Server et WebLogic Express version 7.0, ayant une mise à jour antérieure au Service Pack 7.

3 Résumé

Plusieurs vulnérabilités ont été identifiées dans les produits BEA WebLogic. Ils permettraient à une personne malveillante de contourner de diverses manières la politique de sécurité.

4 Description

Plusieurs vulnérabilités ont été identifiées dans les produits BEA WebLogic. 23 sont citées sur le site de l'éditeur. Parmi celles-ci :

- le service de démarrage et d'arrêt du serveur par les utilisateurs ayant un rôle `Admin` et Operator ne serait pas suffisamment contrôlé ;
- les sites pourraient, sous certaines conditions, diffuser de l'information contextuelle concernant le réseau interne, tels la configuration du NAT, les adresses IPs des machines ou du serveur DNS ;
- la confidentialité SSL pourrait être contournée par un utilisateur distant, afin de récupérer des données en clair ;
- les certificats clients ne seraient pas correctement validés, lorsque les connexions sont mises en cache par le serveur ;
- le module de WebLogic Server pour Apache ne manipulerait pas correctement certaines erreurs, pouvant provoquer l'interruption du service Apache ;
- les requêtes HTTP ne seraient pas vérifiées de manière correcte ; une personne malveillante pourrait donc envoyer des paquets spécialement construits, afin de récupérer des données de requêtes HTTP précédentes ;
- etc.

5 Solution

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

6 Documentation

- Avis de sécurité BEA du 16 janvier 2007 :
  http://dev2dev.bea.com/advisoriesnotifications/index.html
- Référence CVE CVE-2007-0408 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0408
- Référence CVE CVE-2007-0409 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0409
- Référence CVE CVE-2007-0410 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0410
- Référence CVE CVE-2007-0411 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0411
- Référence CVE CVE-2007-0412 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0412
- Référence CVE CVE-2007-0413 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0413
- Référence CVE CVE-2007-0414 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0414
- Référence CVE CVE-2007-0415 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0415
- Référence CVE CVE-2007-0416 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0416
- Référence CVE CVE-2007-0417 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0417
- Référence CVE CVE-2007-0418 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0418
- Référence CVE CVE-2007-0419 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0419
- Référence CVE CVE-2007-0420 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0420
- Référence CVE CVE-2007-0421 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0421

- Référence CVE CVE-2007-0422 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0422
- Référence CVE CVE-2007-0423 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0423
- Référence CVE CVE-2007-0424 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0424
- Référence CVE CVE-2007-0425 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0425
- Référence CVE CVE-2007-0426 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0426

Gestion détaillée du document

23 janvier 2007 version initiale.