Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 septembre 2004
N° CERTA-2004-AVI-321

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans BEA WebLogic

Gestion du document

Référence	CERTA-2004-AVI-321
Titre	Multiples vulnérabilités dans BEA WebLogic
Date de la première version	17 septembre 2004
Date de la dernière version	–
Source(s)	Avis 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

- Contournement de la politique de sécurité ;
- élévation de privilèges ;
- diffusion d'informations confidentielles ;
- déni de service.

2 Systèmes affectés

- BEA WebLogic Express versions 6.x ;
- BEA WebLogic Express versions 7.x ;
- BEA WebLogic Express versions 8.x ;
- BEA WebLogic Server 6.x ;
- BEA WebLogic Server 7.x ;
- BEA WebLogic Server 8.x.

3 Résumé

De multiples vulnérabilités ont été découvertes dans BEA WebLogic. Ces vulnérabilités permettent à un utilisateur mal intentionné de réaliser un déni de service, de contourner la politique de sécurité ou encore de récupérer des informations confidentielles sur le système vulnérable.

4 Description

- Un utilisateur mal intentionné peut récupérer des informations confidentielles ou réaliser un déni de service sur l'arborescence JNDI (Java Naming and Directory Interface) par le biais d'un objet malicieux en utilisant une vulnérabilité liée à une mauvaise protection sur cette arborescence.
- Certaines commandes reservées pour les administrateurs weblogic.Admin peuvent être exécutées par un utilisateur mal intentionné sans que celui-ci soit authentifié comme administrateur sur le système. Cette vulnérabilité n'affecte pas les logiciels BEA WebLogic Express 6.x et BEA WebLogic Server 6.x.
- Une vulnérabilité présente dans l'installation du logiciel peut être utilisée par un utilisateur mal intentionné pour accèder aux ressources du système. Les logiciels installés sur les plates-formes Windows ne sont pas affectés par cette vulnérabilité.
- Des mots de passe écrits en clair dans des utilitaires en ligne de commande peuvent être relus par un utilisateur local mal intentionné pour élever ses privilèges.
- Une vulnérabilité sur les plates-formes linux permet à un utilisateur local mal intentionné de relire le mot de passe de l'administrateur au moment du redémarrage de la machine.
- Un utilisateur mal intentionné, via une requête HTTP malicieusement construite, peut récupérer le numéro de version du serveur BEA WebLogic.
- Une vulnérabilité dans BEA WebLogic peut entraîner l'arrêt de l'application dans un mode dégradé et permettre à un utilisateur mal intentionné de compromettre le système. Cette vulnérabilité n'affecte pas les logiciels BEA WebLogic Express 6.x et BEA WebLogic Server 6.x.
- Des restrictions insuffisantes sur les comptes utilisateur qui sont désactivés peuvent être exploitées par un utilisateur mal intentionné. Cette vulnérabilité n'est exploitable que si le serveur d'authentification Active Directory LDAP est utilisé. Cette vulnérabilité n'affecte pas les logiciels BEA WebLogic Express 6.x et BEA WebLogic Server 6.x.
- Des informations de configuration et des données confidentielles peuvent être envoyées en clair et être récupérées par un utilisateur mal intentionné pour compromettre le système. Cette vulnérabilité n'affecte pas les logiciels BEA WebLogic Express 6.x et BEA WebLogic Server 6.x.

5 Solution

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

6 Documentation

- Site internet de BEA :
  http://www.bea.com
- Avis de sécurité BEA BEA04-65 :
  http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BE04-65.00.jsp
- Avis de sécurité BEA BEA04-66 :
  http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BE04-66.00.jsp
- Avis de sécurité BEA BEA04-67 :
  http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BE04-67.00.jsp
- Avis de sécurité BEA BEA04-68 :
  http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BE04-68.00.jsp
- Avis de sécurité BEA BEA04-69 :
  http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BE04-69.00.jsp

- Avis de sécurité BEA BEA04-70 :
  http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BE04-70.00.jsp
- Avis de sécurité BEA BEA04-71 :
  http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BE04-71.00.jsp
- Avis de sécurité BEA BEA04-72 :
  http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BE04-72.00.jsp
- Avis de sécurité BEA BEA04-73 :
  http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BE04-73.00.jsp

Gestion détaillée du document

17 septembre 2004 version initiale.