



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 26 août 2005
N° CERTA-2005-AVI-201-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités sur 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-2005-AVI-201>

Gestion du document

Référence	CERTA-2005-AVI-201-001
Titre	Multiples vulnérabilités sur BEA Weblogic
Date de la première version	09 juin 2005
Date de la dernière version	26 août 2005
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

- Contournement de la politique de sécurité ;
- déni de service ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- BEA Weblogic Express 6.x ;
- BEA Weblogic Express 7.x ;
- BEA Weblogic Express 8.x ;
- BEA Weblogic Portal 8.x ;
- BEA Weblogic Server 6.x ;
- BEA Weblogic Server 7.x ;
- BEA Weblogic Server 8.x.

3 Résumé

Multiples vulnérabilités présentes dans BEA Weblogic peuvent être exploitées par un utilisateur mal intentionné pour obtenir de l'information sensible ou encore réaliser un déni de service sur le système vulnérable.

4 Description

- Une vulnérabilité a été découverte sur `Weblogic Express/Server 8.1 SP2/SP3` permettant à un utilisateur mal intentionné de limiter ou de réinitialiser les connexions JDBC (Java Database Connectivity) (CAN-2005-1742).
- Une vulnérabilité dans le traitement des exceptions est présente sur `Weblogic Express/Server 8.1 SP3` et `Weblogic Express/Server 7.0 SP5`. Cette vulnérabilité permet à un utilisateur mal intentionné de réaliser un déni de service du service vulnérable (CAN-2005-1743).
- Une vulnérabilité sur `Weblogic Express/Server 7.0 SP5` permet à un utilisateur de se reconnecter à une application web ayant changé ses contraintes de sécurité sans s'authentifier de nouveau (CERTA-2005-1744).
- Une vulnérabilité sur `Weblogic Portal 8.1 SP3` permet de visualiser le mot de passe en clair lors d'un échec de connexion (CAN-2005-1745).
- Une vulnérabilité dans le traitement de l'identifiant de session sur `Weblogic Express/Server 7.0 SP5` s'exécutant sur une grappe permet à un utilisateur mal intentionné de créer un ralentissement du cluster, via un identifiant malicieusement construit (CAN-2005-1746).
- Une vulnérabilité de type « cross site scripting » est présente sur `Weblogic Express/Server 6.1 SP7`, `Weblogic Express/Server 7.0 SP6` et `Weblogic Express et Server 8.1 SP4` (CAN-2005-1747).
- Une vulnérabilité sur le serveur LDAP sur `Weblogic Express/Server 8.1 SP4` et `Weblogic Express/Server 7.0 SP5` permet à un utilisateur mal intentionné d'obtenir des informations sur les utilisateurs de la base ou de réaliser un déni de service sur le serveur vulnérable (CAN-2005-1748).
- Une vulnérabilité de type débordement de mémoire est présente sur `Weblogic Express/Server 6.1 SP4`. Cette vulnérabilité peut être exploitée pour réaliser un déni de service sur le système vulnérable (CAN-2005-1749).

5 Solution

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

6 Documentation

- Bulletin de sécurité BEA 125
<http://dev2dev.bea.com/pub/advisory/125>
- Bulletin de sécurité BEA 126
<http://dev2dev.bea.com/pub/advisory/126>
- Bulletin de sécurité BEA 127
<http://dev2dev.bea.com/pub/advisory/127>
- Bulletin de sécurité BEA 128
<http://dev2dev.bea.com/pub/advisory/128>
- Bulletin de sécurité BEA 129
<http://dev2dev.bea.com/pub/advisory/129>
- Bulletin de sécurité BEA 135
<http://dev2dev.bea.com/pub/advisory/135>
- Bulletin de sécurité BEA 131
<http://dev2dev.bea.com/pub/advisory/131>
- Bulletin de sécurité BEA 132
<http://dev2dev.bea.com/pub/advisory/132>
- Référence CVE CAN-2005-1742
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1742>
- Référence CVE CAN-2005-1743
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1743>
- Référence CVE CAN-2005-1744
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1744>

- Référence CVE CAN-2005-1745
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1745>
- Référence CVE CAN-2005-1746
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1746>
- Référence CVE CAN-2005-1747
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1747>
- Référence CVE CAN-2005-1748
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1748>
- Référence CVE CAN-2005-1749
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1749>

Gestion détaillée du document

09 juin 2005 version initiale ;

26 août 2005 modification du correctif pour la vulnérabilité de type *Cross Site Scripting*.