



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-037-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités de BEA AquaLogic

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-2007-AVI-037>

Gestion du document

Référence	CERTA-2007-AVI-037-001
Titre	Vulnérabilités de BEA AquaLogic
Date de la première version	18 janvier 2007
Date de la dernière version	23 janvier 2007
Source(s)	Mises à jour 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

- Contournement de la politique de sécurité ;
- atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- AquaLogic Service Bus 2.0, 2.1 et 2.5 ;
- AquaLogic Enterprise Security 2.0, jusqu'au Service Pack 2 ;
- AquaLogic Enterprise Security 2.1, jusqu'au Service Pack 1 ;
- AquaLogic Enterprise Security 2.2.

3 Description

BEA est une suite de produits pour gérer les services au sein d'un environnement hétérogène, ou SOA (pour *Service-Oriented Architecture*). Plusieurs vulnérabilités ont été identifiées :

- le service *proxy* ne manipulerait pas correctement certaines requêtes, et permettrait donc de contourner la politique d'accès autorisée par BEA AquaLogic Service Bus ;

- les utilisateurs ayant un compte désactivé mais non supprimé pourraient, sous certaines conditions, continuer à se connecter au serveur BEA AquaLogic Enterprise Security.

Ces vulnérabilités semblent nécessiter un serveur d'authentification Active Directory LDAP pour être exploitable.

4 Solution

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

5 Documentation

- Avis de sécurité BEA dev2dev :
<http://dev2dev.bea.com/advisoriesnotifications/index.html>
- Référence CVE CVE-2007-0432 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0432>
- Référence CVE CVE-2007-0433 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0433>
- Référence CVE CVE-2007-0434 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0434>

Gestion détaillée du document

18 janvier 2007 version initiale.

23 janvier 2007 ajout des références CVE.