



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 08 août 2008
N° CERTA-2008-AVI-394

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Oracle BEA WebLogic Server

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-2008-AVI-394>

Gestion du document

Référence	CERTA-2008-AVI-394
Titre	Vulnérabilité dans Oracle BEA WebLogic Server
Date de la première version	08 août 2008
Date de la dernière version	–
Source(s)	CVE-2008-3257
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

- Exécution de code arbitraire à distance ;
- déni de service à distance.

2 Systèmes affectés

Oracle BEA WebLogic Server, versions 5.x à 10.x, sauf la version 10.3.

3 Résumé

Une vulnérabilité de *Oracle BEA WebLogic Server* permet à un utilisateur malveillant de réaliser un déni de service à distance et d'exécuter du code arbitraire à distance.

4 Description

Une vulnérabilité existe dans le connecteur *Apache* du serveur *Oracle BEA WebLogic Server*. Certaines requêtes excessivement longues, de type POST, peuvent provoquer un débordement de pile. Ce débordement est

exploitable pour réaliser un déni de service à distance et, dans certaines conditions, exécuter des commandes sur le serveur vulnérable.

Une preuve de faisabilité est disponible sur l'Internet.

5 Solution

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

6 Documentation

- Bulletin de sécurité Oracle du 08 août 2008 :
https://support.bea.com/application_content/product_portlets/securityadvisories/2793.html
- Document du CERTA CERTA-2008-ALE-011 du 29 juillet 2008 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-ALE-011/index.html>
- Référence CVE CVE-2008-3257 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3257>

Gestion détaillée du document

08 août 2008 version initiale.