



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 30 janvier 2006
N° CERTA-2006-AVI-054

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans 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-2006-AVI-054>

Gestion du document

Référence	CERTA-2006-AVI-054
Titre	Multiples vulnérabilités dans BEA Weblogic
Date de la première version	30 janvier 2006
Date de la dernière version	–
Source(s)	Multiples bulletins de sécurité de BEA Systems
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

- Dénis 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 Portal 8.x ;
- BEA WebLogic Express 6.x ;
- BEA WebLogic Express 7.x ;
- BEA WebLogic Express 8.x ;
- BEA WebLogic Express 9.x ;
- BEA WebLogic Server 6.x ;
- BEA WebLogic Server 7.x ;
- BEA WebLogic Server 8.x ;
- BEA WebLogic Server 9.x ;

3 Description

De nombreuses vulnérabilités affectant certains produits BEA WebLogic peuvent être exploitées à distance par un utilisateur mal intentionné de manière à réaliser plusieurs actions pouvant conduire à la compromission du système.

4 Solution

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

5 Documentation

- Bulletin de sécurité BEA Systems BEA06-108 du 24 janvier 2006 :
<http://dev2dev.bea.com/pub/advisory/165>
- Bulletin de sécurité BEA Systems BEA06-109 du 24 janvier 2006 :
<http://dev2dev.bea.com/pub/advisory/166>
- Bulletin de sécurité BEA Systems BEA06-110 du 24 janvier 2006 :
<http://dev2dev.bea.com/pub/advisory/167>
- Bulletin de sécurité BEA Systems BEA06-111 du 24 janvier 2006 :
<http://dev2dev.bea.com/pub/advisory/168>
- Bulletin de sécurité BEA Systems BEA06-112 du 24 janvier 2006 :
<http://dev2dev.bea.com/pub/advisory/169>
- Bulletin de sécurité BEA Systems BEA06-113 du 24 janvier 2006 :
<http://dev2dev.bea.com/pub/advisory/170>
- Bulletin de sécurité BEA Systems BEA06-114 du 24 janvier 2006 :
<http://dev2dev.bea.com/pub/advisory/171>
- Bulletin de sécurité BEA Systems BEA06-115 du 24 janvier 2006 :
<http://dev2dev.bea.com/pub/advisory/172>
- Bulletin de sécurité BEA Systems BEA06-116 du 24 janvier 2006 :
<http://dev2dev.bea.com/pub/advisory/173>
- Bulletin de sécurité BEA Systems BEA06-117 du 24 janvier 2006 :
<http://dev2dev.bea.com/pub/advisory/174>
- Bulletin de sécurité BEA Systems BEA06-118 du 24 janvier 2006 :
<http://dev2dev.bea.com/pub/advisory/175>
- Bulletin de sécurité BEA Systems BEA06-119 du 24 janvier 2006 :
<http://dev2dev.bea.com/pub/advisory/176>
- Référence CVE CAN-2006-0421 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-0421>
- Référence CVE CAN-2006-0422 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-0422>
- Référence CVE CAN-2006-0423 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-0423>
- Référence CVE CAN-2006-0424 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-0424>
- Référence CVE CAN-2006-0425 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-0425>
- Référence CVE CAN-2006-0426 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-0426>
- Référence CVE CAN-2006-0427 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-0427>
- Référence CVE CAN-2006-0428 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-0428>

- Référence CVE CAN-2006-0429 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-0429>
- Référence CVE CAN-2006-0430 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-0430>
- Référence CVE CAN-2006-0431 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-0431>
- Référence CVE CAN-2006-0432 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-0432>

Gestion détaillée du document

30 janvier 2006 version initiale.