



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 12 juillet 2002  
N° CERTA-2002-AVI-149

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité des Web Applications

---

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-2002-AVI-149>

---

### Gestion du document

Référence	CERTA-2002-AVI-149
Titre	Vulnérabilité des Web Applications
Date de la première version	12 juillet 2002
Date de la dernière version	–
Source(s)	Avis de sécurité Westpoint
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

Divulgateion de données.

## 2 Systèmes affectés

De nombreux serveurs web supportant les « Web Applications » comme par exemple :

- serveur Sybase versions antérieures à la version 4.1 ;
- serveur Oracle versions antérieures à la version 9.0.2 ;
- serveur Jrun versions 3.0, 3.1 et 4.0 ;
- serveur Orion versions antérieures à la version 1.5.4 ;
- serveur HPAS version 8.0 ;
- serveur Jo Webserver versions antérieures à la version 1.0b7.

## 3 Résumé

Une vulnérabilité présente dans de nombreux moteurs de « servlets » permet à un utilisateur mal intentionné d'accéder aux fichiers présents dans le répertoire WEB-INF. Les servlets sont l'équivalent des CGI (Common Gateway Interfaces) dans le langage Java.

## 4 Description

Une « Web Application » est une collection de fichiers regroupés dans un fichier archive .war. Ce fichier archive est toujours organisé selon le même principe : des fichiers JSP (Java Server Pages), des fichiers html, d'autres fichiers et un répertoire WEB-INF contenant les fichiers nécessaires au fonctionnement des servlets mais réservé en lecture et en écriture aux développeurs.

Une vulnérabilité présente dans de nombreux moteurs de « servlets » permet à utilisateur mal intentionné d'accéder au contenu de ce répertoire, et donc aux fichiers de configuration des servlets ou encore aux informations de sessions des utilisateurs.

## 5 Solution

Appliquer le correctif correspondant à votre serveur Web (cf section documentation).

## 6 Documentation

- Site de Sybase pour la version 4.1 de Sybase EAServer :  
<http://www.sybase.com>
- Avis de sécurité de Macromedia :  
<http://www.macromedia.com/v1/handlers/index.cfm?ID=23164>
- avis de sécurité de Westpoint :  
<http://www.westpoint.ltd.uk/advisories/wp-02-2002.txt>

## Gestion détaillée du document

12 juillet 2002 version initiale.