

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité des interpréteurs XML de serveurs WEB (SOAP)

---

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-2003-AVI-215>

---

### Gestion du document

Référence	CERTA-2003-AVI-215
Titre	Vulnérabilité des interpréteurs XML de serveurs WEB (SOAP)
Date de la première version	18 décembre 2003
Date de la dernière version	–
Source(s)	Liste de diffusion BugTraq
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

Déni de service.

## 2 Systèmes affectés

- IBM WebSphere 5.0.0, 5.0.1, 5.0.2, 5.0.2.1 ;
- Macromedia Coldfusion MX 6.0, 6.1 ;
- Macromedia JRun 4.

## 3 Résumé

Une vulnérabilité présente sur les interpréteurs XML des serveurs WEB affectés permet à un utilisateur mal intentionné de réaliser un déni de service du système.

## 4 Description

Une vulnérabilité présente sur les interpréteurs XML des serveurs WEB utilisant SOAP permet à un utilisateur mal intentionné de réaliser un déni de service.

Par le biais d'une requête SOAP malicieusement construite, un utilisateur mal intentionné peut consommer toutes les ressources CPU du système et réaliser un déni de service.

## **5 Solution**

Appliquer les correctifs disponibles (cf section documentation).

## **6 Documentation**

- Avis de sécurité IBM :  
<http://www-1.ibm.com/support/docview.wss?rs=180&context=SSEQTP&q=PQ81278&uid=swg24005943>
- Correctif IBM Websphere de l'interpréteur XML :  
<ftp://ftp.software.ibm.com/software/websphere/appserv/support/fixes/PQ81278/>
- Avis de sécurité Macromedia :  
[http://www.macromedia.com/devnet/security/security\\_zone/mpsb03-07.html](http://www.macromedia.com/devnet/security/security_zone/mpsb03-07.html)
- Correctif de l'interpréteur XML de macromédia :  
<http://download.macromedia.com/pub/security/mpsb03-07.zip>
- Avis de sécurité sur la liste de diffusion BugTraq :  
<http://www.securityfocus.com/archive/1/346992>

## **Gestion détaillée du document**

**18 décembre 2003** version initiale.