

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans Apache Tomcat

---

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-148>

---

### Gestion du document

Référence	CERTA-2002-AVI-148
Titre	Multiples vulnérabilités dans Apache Tomcat
Date de la première version	12 juillet 2002
Date de la dernière version	–
Source(s)	Avis de sécurité de 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

- Exécution de code arbitraire ;
- divulgation du répertoire d'installation.

## 2 Systèmes affectés

Apache Tomcat 4.0.3 sous Windows NT4.0, Windows 2000 et Linux.

## 3 Résumé

Des vulnérabilités du module tomcat d'Apache permettent la divulgation d'informations ou l'exécution de scripts sur un poste client.

## 4 Description

Tomcat est un module d'Apache permettant l'utilisation des servlet java ou des pages javaserver.  
Tomcat ne filtre pas correctement les requêtes qu'il reçoit, un lien pointant vers ce serveur peut donc contenir un

script.

Le serveur recevant ce type de requête va engendrer une page d'erreur incluant le script contenu dans la requête. Ce script s'exécutera sur le poste client muni des droits de l'utilisateur ayant démarré le navigateur.

Un autre type de requête permet de découvrir le répertoire d'installation du serveur.

## 5 Contournement provisoire

Le servlet `invoker`, présent dans le répertoire `/servlet/`, permettant d'exécuter des servlets anonymes non définis dans le fichier `web.xml`, doit être désactivé.

`web.xml` se trouve généralement dans : `/tomcat_install_dir/conf/web.xml`

Une mise à jour vers la version 4.1.3 beta corrige la vulnérabilité qui permet à un utilisateur mal intentionné de découvrir le répertoire d'installation du module Tomcat.

Cette mise à jour est disponible sur le site :

<http://jakarta.apache.org/tomcat/>

## 6 Documentation

- Note d'information du CERTA concernant le Cross Site Scripting : CERTA-2002-INF-001
- Avis de Westpoint :  
<http://www.westpoint.ltd.uk/advisories/wp-02-0008.txt>

## Gestion détaillée du document

12 juillet 2002 version initiale.