

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité 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-2007-AVI-157>

---

### Gestion du document

Référence	CERTA-2007-AVI-157
Titre	Vulnérabilité dans Apache Tomcat
Date de la première version	04 avril 2007
Date de la dernière version	–
Source(s)	bulletins de sécurité Apache Tomcat
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

Contournement de la politique de sécurité.

## 2 Systèmes affectés

- Apache Tomcat versions antérieures à 5.5.22 ;
- Apache Tomcat versions antérieures à 6.0.10.

## 3 Résumé

Une vulnérabilité présente dans Apache Tomcat permet de contourner la politique de sécurité.

## 4 Description

Sous certaines conditions, comme l'utilisation d'un mode mandataire (*proxy*) tel que : `mod_proxy`, `mod_rewrite` ou `mod_jk`, un manque de contrôle de l'adresse réticulaire (*URL*) permet à un utilisateur malveillant d'accéder à des informations présentes sur le serveur par le biais d'une requête spécialement conçue.

## 5 Solution

Les versions 5.5.22 et 6.0.10 d'Apache Tomcat corrigent le problème. Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

## 6 Documentation

- Bulletin de sécurité Apache Tomcat 5.x :  
<http://tomcat.apache.org/security-5.html>
- Bulletin de sécurité Apache Tomcat 6.x :  
<http://tomcat.apache.org/security-6.html>
- Référence CVE CVE-2007-0450 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0450>

## Gestion détaillée du document

04 avril 2007 version initiale.