

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de 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-267>

---

## Gestion du document

Référence	CERTA-2007-AVI-267
Titre	Vulnérabilité de Tomcat
Date de la première version	18 juin 2007
Date de la dernière version	–
Source(s)	Bulletin 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

Exécution de code arbitraire à distance.

## 2 Systèmes affectés

*Apache Tomcat*, versions 4.0.x, 4.1.x, 5.0.x, 5.5.x, 6.0.x

## 3 Résumé

Une vulnérabilité dans les applications d'administration de *Tomcat* et dans des exemples d'application permet d'exécuter du code à distance sur les postes des utilisateurs.

## 4 Description

Une vulnérabilité est présente dans des fichiers JSP d'exemples d'application et dans les applications d'administration de *Tomcat*, *Manager* et *Host Manager*. Le manque de filtrage des données entrées permet de réaliser des injections de code indirectes (*cross-site scripting*). Le code est exécuté sur le poste de l'utilisateur connecté à l'application vulnérable, avec les droits octroyés au site.

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité *Apache Tomcat* :  
<http://www.apache.org/security-6.html>  
<http://www.apache.org/security-5.html>  
<http://www.apache.org/security-4.html>
- Référence CVE CVE-2007-2449 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2449>
- Référence CVE CVE-2007-2450 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2450>

## Gestion détaillée du document

**18 juin 2007** version initiale.