

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités 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-362>

---

### Gestion du document

Référence	CERTA-2007-AVI-362
Titre	Multiples vulnérabilités de Tomcat
Date de la première version	16 août 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité du projet 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

- Injection de code indirecte (*cross site scripting*);
- contournement de la politique de sécurité.

## 2 Systèmes affectés

*Tomcat*, versions antérieures à 6.0.14.

## 3 Résumé

Plusieurs vulnérabilités du moteur de *servlets Tomcat* permettent à un utilisateur malveillant de réaliser des injections de code indirectes ou de voler des identifiants de session.

## 4 Description

Plusieurs vulnérabilités sont présentes dans le moteur de *servlets Tomcat* :

- (CVE-2007-2449 et CVE-2007-3383) les exemples de JSP livrés avec le logiciel ne filtrent pas les données entrées par l'utilisateur. Cette absence de filtrage permet la réalisation malveillante d'injections de code indirectes (*cross site scripting*);

- (CVE-2007-2450) les applications web *Manager* et *Host Manager* ne filtrent pas les données entrées par l'utilisateur. Cette absence de filtrage permet la réalisation malveillante d'injections de code indirectes (*cross site scripting*);
- (CVE-2007-3382) le moteur *Tomcat* ne traite pas de manière correcte le caractère apostrophe ( ' ) quand il sert de délimiteur dans des *cookies*. Dans certaines conditions, cette erreur permet la divulgation de l'identifiant de session et le détournement de cette session;
- (CVE-2007-3385) le moteur *Tomcat* ne traite pas de manière correcte la séquence de caractères \ " utilisée des *cookies*. Dans certaines conditions, cette erreur permet la divulgation de l'identifiant de session et le détournement de cette session;
- (CVE-2007-3386) la *servlet Host Manager* ne filtre pas les données entrées par l'utilisateur. Cette absence de filtrage permet la réalisation malveillante d'injections de code indirectes (*cross site scripting*).

## 5 Solution

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

## 6 Documentation

- Bulletins de sécurité du projet Tomcat :  
<http://tomcat.apache.org/security-6.html>  
<http://tomcat.apache.org/security-5.html>
- Référence CVE CVE-2007-1355 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1355>
- Référence CVE CVE-2007-2449 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2449>
- Référence CVE CVE-2007-3383 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3383>
- Référence CVE CVE-2007-2450 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2450>
- Référence CVE CVE-2007-3382 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3382>
- Référence CVE CVE-2007-3385 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3385>
- Référence CVE CVE-2007-3386 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3386>

## Gestion détaillée du document

16 août 2007 version initiale.