



Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : 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-2010-AVI-567>

Gestion du document

Référence	CERTA-2010-AVI-567
Titre	Vulnérabilités dans Apache Tomcat
Date de la première version	29 novembre 2010
Date de la dernière version	–
Source(s)	Liste des vulnérabilités affectant Apache Tomcat 7.x Liste des Vulnérabilités affectant Apache Tomcat 6.x
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 à distance.

2 Systèmes affectés

- Apache Tomcat 7.0.0 à 7.0.4 ;
- Apache Tomcat 6.0.12 à 6.0.29.

3 Résumé

Des vulnérabilités ont été découvertes dans Apache Tomcat. Elles permettent à un utilisateur de faire de l'injection de code indirecte à distance.

4 Description

Apache Tomcat n'assainit pas correctement les entrées passées via les paramètres *short* et *order by* dans *sessionsList.jsp*. Cette vulnérabilité peut être exploitée par un utilisateur pour faire de l'injection de code indirecte à distance.

5 Solution

Les versions corrigées sont disponibles sur le serveur *subversion* de Apache, en attendant la sortie des versions 7.0.5 et 6.0.30. Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Liste des vulnérabilités affectant Apache Tomcat 7 :
<http://tomcat.apache.org/security-7.html>
- Liste des vulnérabilités affectant Apache Tomcat 6 :
<http://tomcat.apache.org/security-6.html>
- Référence CVE CVE-2010-4172 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4172>

Gestion détaillée du document

29 novembre 2010 version initiale.