

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-2012-AVI-025>

---

### Gestion du document

Référence	CERTA-2012-AVI-025
Titre	Vulnérabilité dans Apache Tomcat
Date de la première version	18 janvier 2012
Date de la dernière version	–
Source(s)	Notes de mise à jour 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 ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

- Apache Tomcat versions 6.0.30 à 6.0.33 ;
- Apache Tomcat versions 7.0.0 à 7.0.21.

## 3 Résumé

Une vulnérabilité portant atteinte à la confidentialité des données et permettant un contournement de la politique de sécurité a été corrigée dans Apache Tomcat.

## 4 Description

Une vulnérabilité dans Apache Tomcat provoque une fuite de données permettant à un utilisateur malintentionné de contourner la politique de sécurité. Une partie de la mémoire utilisée par Apache Tomcat pour stocker

les requêtes n'est pas correctement recyclée. La réutilisation de cette mémoire provoque, sous certaines conditions, une fuite d'information entre deux requêtes.

## **5 Solution**

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation). Les versions 6.0.35 et 7.0.22 corrigent le problème.

## **6 Documentation**

- Notes de mise à jour de sécurité Apache Tomcat du 17 janvier 2012 :  
<http://tomcat.apache.org/security-6.html>  
<http://tomcat.apache.org/security-7.html>
- Rapport de bug Apache Tomcat du 22 septembre 2011 :  
[https://issues.apache.org/bugzilla/show\\_bug.cgi?id=51872](https://issues.apache.org/bugzilla/show_bug.cgi?id=51872)
- Référence CVE CVE-2011-3375 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3375>

## **Gestion détaillée du document**

**18 janvier 2012** version initiale.