

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-2011-AVI-485>

Gestion du document

Référence	CERTA-2011-AVI-485
Titre	Vulnérabilité dans Apache Tomcat
Date de la première version	31 août 2011
Date de la dernière version	–
Source(s)	
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 l'intégrité des données ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

Apache Tomcat, versions 5.5.x, 6.0.x et 7.0.x.

3 Résumé

Une vulnérabilité dans Apache Tomcat permet à un utilisateur malveillant de contourner la politique de sécurité et de porter atteinte à l'intégrité et à la confidentialité de données.

4 Description

Une vulnérabilité dans Apache Tomcat affecte le traitement du protocole AJP (*Apache JServ Protocol*).

Elle permet à un utilisateur malveillant d'insérer une adresse IP de client ou le nom d'un utilisateur authentifié, et de provoquer le mélange des réponses de requêtes d'utilisateurs différents.

5 Solution

Les correctifs sont les suivants selon les branches :

- révision 1162960, puis version 5.5.34 dès publication ;
- révision 1162959, puis version 6.0.34 dès publication ;
- révision 1162958, puis version 7.0.21 dès publication.

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

6 Documentation

- Annonces de versions Apache Tomcat du 29 août 2011 :
<http://tomcat.apache.org/security-5.html>
<http://tomcat.apache.org/security-6.html>
<http://tomcat.apache.org/security-7.html>
- Référence CVE CVE-2011-3190 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3190>

Gestion détaillée du document

31 août 2011 version initiale.