

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-2008-AVI-416>

Gestion du document

Référence	CERTA-2008-AVI-416
Titre	Vulnérabilité dans Apache Tomcat
Date de la première version	14 août 2008
Date de la dernière version	–
Source(s)	Bulletin du NIST CVE-2008-2938 du 12 août 2008
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 6.0.x.

3 Résumé

Une vulnérabilité dans Apache Tomcat permet à un utilisateur distant malintentionné de contourner la politique de sécurité et de porter atteinte à la confidentialité des données présentes sur le serveur vulnérable.

4 Description

Une vulnérabilité de type traversée de répertoire peut être exploitée lorsque l'option `allowLinking` et la prise en charge de l'encodage UTF-8 sont activés sur le serveur.

Un utilisateur distant malveillant peut exploiter cette vulnérabilité, au moyen d'adresses réticulaires spécialement construites, afin porter atteinte à la confidentialité des données.

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://tomcat.apache.org/security-6.html>
- Bulletin du NIST CVE-2008-2938 du 12 août 2008 :
<http://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-2938>
- Référence CVE CVE-2008-2938 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2938>

Gestion détaillée du document

14 août 2008 version initiale.