

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité 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-345>

Gestion du document

| | |
|-----------------------------|---------------------------------------|
| Référence | CERTA-2007-AVI-345 |
| Titre | Vulnérabilité de Tomcat |
| Date de la première version | 06 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

Exécution de code arbitraire à distance.

2 Systèmes affectés

Tomcat, version 3.x.

3 Résumé

Une mauvaise gestion des messages d'erreur permet à un utilisateur malintentionné d'exécuter un code arbitraire à distance.

4 Description

Lorsque Tomcat retourne une page d'erreur, les entrées ayant provoqué l'erreur ne sont pas filtrées. Cela permet à un utilisateur malveillant de provoquer une injection de code indirecte (*XSS*, *cross site scripting*).

Des preuves de faisabilité existent sur l'Internet.

5 Solution

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

6 Documentation

- Bulletin de sécurité du projet Tomcat :
<http://tomcat.apache.org/security-3.html>
- Référence CVE CVE-2007-3384 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3384>

Gestion détaillée du document

06 août 2007 version initiale.