

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples 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-2011-AVI-081>

Gestion du document

Référence	CERTA-2011-AVI-081-001
Titre	Multiples vulnérabilités dans Apache Tomcat
Date de la première version	10 février 2011
Date de la dernière version	01 août 2011
Source(s)	Listes des vulnérabilités affectant Apache Tomcat 5, 6 et 7
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 ;
- déni de service à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- Apache Tomcat 5 versions antérieures à 5.5.32 ;
- Apache Tomcat 6 versions antérieures à 6.0.32 ;
- Apache Tomcat 7 versions antérieures à 7.0.8.

3 Résumé

Plusieurs vulnérabilités ont été corrigées sur les serveurs Apache Tomcat versions 5, 6 et 7.

4 Description

Plusieurs vulnérabilités ont été corrigées sur les serveurs Apache Tomcat. Elles peuvent notamment être exploitées par des utilisateurs locaux pour contourner la politique de sécurité, et par des attaquants distants pour réaliser un déni de service ou une injection de code indirecte.

5 Solution

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>
- Liste des vulnérabilités affectant Apache Tomcat 5 :
<http://tomcat.apache.org/security-5.html>
- Bulletin de sécurité IBM swg21507512 du 29 juillet 2011 :
<http://www-01.ibm.com/support/docview.wss?uid=swg21507512>
- Référence CVE CVE-2010-3718 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3718>
- Référence CVE CVE-2010-4476 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4476>
- Référence CVE CVE-2011-0013 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0013>
- Référence CVE CVE-2011-0534 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0534>

Gestion détaillée du document

10 février 2011 version initiale.

01 août 2011 ajout du bulletin IBM.