

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-2007-AVI-108>

Gestion du document

Référence	CERTA-2007-AVI-108-002
Titre	Vulnérabilité dans Apache Tomcat
Date de la première version	05 mars 2007
Date de la dernière version	01 février 2008
Source(s)	Liste des changements apportés à la version 1.2.21 d'Apache Tomcat Connector
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 ;
- déni de service à distance.

2 Systèmes affectés

- Tomcat JK Web Server Connector 1.2.19 ;
- Tomcat JK Web Server Connector 1.2.20 ;
- Tomcat 4.1.34 ;
- Tomcat 5.5.20.

3 Résumé

Une vulnérabilité présente dans Tomcat JK Web Server Connector permettrait à un utilisateur distant de réaliser un déni de service ou d'exécuter du code arbitraire.

4 Description

Une mauvaise gestion des adresses réticulaires (*URL*) dans la bibliothèque `mod_jk.so` permettrait à un utilisateur distant malintentionné d'exécuter du code arbitraire ou de réaliser un déni de service par le biais d'une adresse réticulaire spécialement conçue.

5 Solution

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

6 Documentation

- Liste des changements apportés à la version 1.2.21 d'Apache Tomcat Connector :
<http://tomcat.apache.org/connectors-doc/miscellaneous/changelog.html>
- Bulletin de sécurité Gentoo GLSA-200703-16 du 16 mars 2007 :
<http://www.gentoo.org/security/en/glsa/glsa-200703-16.xml>
- Bulletin de sécurité Cisco 20080130 du 30 janvier 2008 :
http://www.cisco.com/en/US/products/products_security_advisory09186a0080093f040.shtml#@
- Référence CVE CVE-2007-0774 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0774>

Gestion détaillée du document

05 mars 2007 version initiale.

26 mars 2007 ajout de la référence au bulletin de sécurité Gentoo.

01 février 2008 ajout de la référence au bulletin de sécurité Cisco.