

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du module `mod_jk` du serveur web Apache

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-2002-AVI-269>

Gestion du document

Référence	CERTA-2002-AVI-269
Titre	Vulnérabilité du module <code>mod_jk</code> du serveur web Apache
Date de la première version	16 décembre 2002
Date de la dernière version	–
Source(s)	Avis de sécurité Qualys QSA-2002-12-04
Pièce(s) jointe(s)	Aucune

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

- Déni de service ;
- divulgations d'informations.

2 Systèmes affectés

Tout serveur web Apache (quel que soit le système d'exploitation) possédant la configuration suivante :

- Apache versions 1.3.x,
- module Apache `mod_jk` version 1.2 dialoguant avec le serveur web Java Tomcat en version 4.x.

3 Résumé

Tomcat est un serveur web Java, développé par la fondation Apache, et permettant d'implémenter les technologies *Servlet* (applets Java exécutées sur le serveur) et *JavaServer Pages*.

`mod_jk` est un module pour le serveur Apache permettant à ce dernier de transmettre de façon transparente au moteur Tomcat les requêtes correspondant aux technologies précitées.

Une mauvaise gestion du protocole de communication par ce module permet à un utilisateur mal intentionné de réaliser un déni de service.

4 Description

Le module *mod_jk* n'interprète pas correctement la fonctionnalité «chunk-encoding» du protocole HTTP/1.1. Cette spécification est employée lorsque la taille des données envoyées au serveur n'est pas connue a priori.

Cela induit une dé-synchronisation entre les requêtes envoyées par le module et les réponses du serveur *Tomcat*. Des clients du serveur *Apache* peuvent ainsi recevoir les réponses destinées à d'autres. Par ailleurs, le module peut aller jusqu'à saturer ses mémoires tampons et ne plus offrir aucun service.

5 Solution

Mettre à jour le module *mod_jk* avec une version au moins égale à 1.2.1 :
<http://jakarta.apache.org/builds/jakarta-tomcat-connectors/jk/release/v1.2.1/>

6 Documentation

Avis de sécurité Qualys :
<http://archives.neohapsis.com/archives/bugtraq/2002-12/0045.html>

Gestion détaillée du document

16 décembre 2002 version initiale.