



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
*Agence nationale de la sécurité
des systèmes d'information*
CERTA

Paris, le 29 mai 2007
N° CERTA-2007-AVI-229

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans 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-229>

Gestion du document

Référence	CERTA-2007-AVI-229
Titre	Vulnérabilité dans Tomcat
Date de la première version	29 mai 2007
Date de la dernière version	–
Source(s)	Bulletin de version de Tomcat du 18 mai 2007
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.

2 Systèmes affectés

mod_jk, versions 1.2.22 et antérieures.

Ce composant est livré avec *Tomcat*, versions :

- 4.0.1 à 4.0.6 ;
- 5.0.0 à 5.0.30 ;
- 5.5.0 à 5.5.23.

3 Résumé

Une vulnérabilité de mod_jk permet à un utilisateur malveillant de contourner la politique de sécurité.

4 Description

Une mauvaise gestion du codage des deux points (« .. ») est exploitable par un utilisateur malveillant pour utiliser des ressources auxquelles il ne devrait pas accéder.

5 Solution

La version 1.2.23 de `mod_jk` corrige le problème. Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

Le correctif peut induire des incompatibilités avec le composant `mod_rewrite`.

6 Documentation

- Bulletin de version Tomcat du 18 mai 2007 :
<http://tomcat.apache.org/connectors-doc/news/20070301.html#20070518.1>
- Référence CVE CVE-2007-1860 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1860>

Gestion détaillée du document

29 mai 2007 version initiale.