

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de Tivoli Storage Manager client

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-2009-AVI-178>

Gestion du document

Référence	CERTA-2009-AVI-178
Titre	Multiples vulnérabilités de Tivoli Storage Manager client
Date de la première version	11 mai 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité IBM swg21384389 du 30 avril 2009
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

- Déni de service à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- Tivoli Storage Manager 5.5 client versions antérieures à 5.5.2 ;
- Tivoli Storage Manager 5.4 client versions antérieures à 5.4.2 ;
- Tivoli Storage Manager 5.3 client versions antérieures à 5.3.6.6 ;
- Tivoli Storage Manager 5.2 client versions antérieures à 5.2.5.4 ;
- Tivoli Storage Manager 5.1 client versions antérieures à 5.1.8.3 ;
- Tivoli Storage Manager Express client versions antérieures à 5.3.6.6.

3 Résumé

Plusieurs vulnérabilités de *Tivoli Storage Manager* permettent à un individu malintentionné de contourner la politique de sécurité et de réaliser un déni de service.

4 Description

De multiples vulnérabilités affectent le client de *Tivoli Storage Manager* (ou *TSM*) :

- plusieurs vulnérabilités affectent les interfaces graphiques des clients (Web et Java) et permettent à un individu malveillant d’avoir accès au système de fichiers de la machine disposant du client *TSM* ;
- une vulnérabilité de type homme au milieu (ou *man in the middle*) affectent les versions du client *TSM* fonctionnant sous AIX et Windows. Cette vulnérabilité permet à un individu malintentionné de contourner la politique de sécurité de la machine ;
- la dernière vulnérabilité concerne *Tivoli Storage Manager Agent Client* : un individu distant peut réaliser un déni de service au moyen d’un paquet construit de façon malveillante.

5 Solution

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

6 Documentation

- Bulletin de sécurité IBM swg21384389 du 30 avril 2009 :
<http://www-01.ibm.com/support/docview.wss?uid=swg21384389>
- Référence CVE CVE-2008-4828 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4828>

Gestion détaillée du document

11 mai 2009 version initiale.