

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités de Tivoli

---

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-411>

---

### Gestion du document

Référence	CERTA-2007-AVI-411
Titre	Multiples vulnérabilités de Tivoli
Date de la première version	21 septembre 2007
Date de la dernière version	–
Source(s)	Bulletin IBM 1268775 du 20 septembre 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

- Exécution de code arbitraire à distance ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

IBM Tivoli, versions 5.x.

## 3 Résumé

Des vulnérabilités sur Tivoli Storage Manager ont été publiées. Elle permettent à un utilisateur malveillant d'accéder à des données sensibles ou de provoquer un déni de service à distance, voire d'exécuter du code arbitraire à distance.

## 4 Description

Deux vulnérabilités ont été publiées :

- la première vulnérabilité, non précisée par l'éditeur, permet à un utilisateur malveillant d'accéder à des données sensibles, dans certaines conditions ;

- la deuxième vulnérabilité provient d'une erreur dans le démon Client Acceptor Daemon et peut provoquer un débordement de mémoire. Cette vulnérabilité permet à un utilisateur malveillant de provoquer un déni de service à distance, voire l'exécution d'un code arbitraire à distance.

## **5 Solution**

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

## **6 Documentation**

- Bulletin IBM 1268775 du 20 septembre 2007 :  
<http://www-1.ibm.com/support/docview.wss?uid=swg21268775>

## **Gestion détaillée du document**

**21 septembre 2007** version initiale.