



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 05 novembre 2008  
N° CERTA-2008-AVI-538

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans IBM Tivoli Storage Manager

---

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-2008-AVI-538>

---

### Gestion du document

Référence	CERTA-2008-AVI-538
Titre	Vulnérabilité dans IBM Tivoli Storage Manager
Date de la première version	05 novembre 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité IBM Tivoli numéro 1322623
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

- TSM versions 5.5.0.0 à 5.5.0.7 ;
- TSM versions 5.4.0.0 à 5.4.2.2 ;
- TSM versions 5.3.0.0 à 5.3.6.1 ;
- TSM versions 5.2.0.0 à 5.2.5.2 ;
- TSM versions 5.1.0.0 à 5.1.8.1 ;
- TSM Express toutes versions.

## 3 Résumé

Une vulnérabilité permettant d'effectuer un déni de service à distance ou d'exécuter du code arbitraire à distance a été découverte dans IBM Tivoli Storage Manager.

## 4 Description

Une vulnérabilité a été découverte dans IBM Tivoli Storage Manager. Cette vulnérabilité est due à une erreur au niveau de l'exécutable *dsmcad.exe*. Elle peut être exploitée à distance via un paquet *TCP* spécialement construit afin de réaliser un déni de service ou exécuter du code arbitraire.

## 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 swg21322623 du 30 octobre 2008 :  
<http://www-1.ibm.com/support/docview.wss?uid=swg21322623>
- Référence CVE CVE-2008-4801 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4801>

## Gestion détaillée du document

05 novembre 2008 version initiale.