

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de IBM 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-2005-AVI-252>

---

### Gestion du document

|                             |                             |
|-----------------------------|-----------------------------|
| Référence                   | CERTA-2005-AVI-252          |
| Titre                       | Vulnérabilité de IBM Tivoli |
| Date de la première version | 12 juillet 2005             |
| Date de la dernière version | –                           |
| Source(s)                   | Bulletin IBM 1210334        |
| 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.

## 2 Systèmes affectés

IBM Tivoli Management Framework version 4.x (antérieure à la version 4.1.1) disposant du sous-composant LCF versions 41100 et antérieures.

## 3 Résumé

IBM Tivoli Management Framework propose une interface de gestion à distance des Tivoli Management End-point qui, une fois installés sur des composantes du système d'information, permettent de gérer et de surveiller leur niveau de sécurité.

Le sous-composant LCF gère l'interfaçage réseau de cette solution.

Un problème dans la gestion de certaines connexions au niveau de ce sous-composant provoque un déni de service.

## 4 Description

Si une connexion est établie vers LCF, mais qu'aucun paquet n'est envoyé, le processus génère un message d'erreur, puis se termine, interdisant tout trafic valide.

Il est possible d'identifier une attaque réussie en recherchant une entrée similaire dans les journaux d'évènements :

```
Nov 28 12:00:00 1 lcfcd Terminating for exception: net_recv: bad packet
Nov 28 10:00:00 1 lcfcd Clean Shutdown
```

## 5 Solution

Appliquer le dernier patch LCF (4.1.1-LCF-0020) disponible à l'adresse suivante :  
<http://www-1.ibm.com/support/docview.wss?uid=swg24009815>

## 6 Documentation

IBM:  
<http://www-1.ibm.com/support/docview.wss?uid=swg21210334>

Référence CVS CAN-2005-2170:  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2170>

## Gestion détaillée du document

**12 juillet 2005** version initiale.