

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans 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-2011-AVI-322>

Gestion du document

Référence	CERTA-2011-AVI-322
Titre	Vulnérabilité dans IBM Tivoli
Date de la première version	1 juin 2011
Date de la dernière version	–
Source	Bulletin de sécurité IBM swg21499146 du 30 mai 2011
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.

2 Systèmes affectés

IBM Tivoli, versions 3.x et 4.x

3 Résumé

Une vulnérabilité dans IBM Tivoli permet à un utilisateur malveillant d'exécuter du code arbitraire à distance.

4 Description

Le démon *lcfld* d'IBM Tivoli présente un défaut de vérification de bornes dans une variable. Cette vulnérabilité est exploitable par un utilisateur malveillant authentifié, au moyen d'une requête HTTP spécialement conçue, pour exécuter du 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 de sécurité IBM swg21499146 du 30 mai 2011 :
<http://www-01.ibm.com/support/docview.wss?uid=swg21499146>
- Référence CVE CVE-2011-1220 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1220>

Gestion détaillée du document

1 juin 2011 version initiale.