

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le gestionnaire de base de données IBM DB2

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-2004-AVI-070>

Gestion du document

Référence	CERTA-2004-AVI-070
Titre	Vulnérabilité dans le gestionnaire de base de données IBM DB2
Date de la première version	10 mars 2004
Date de la dernière version	–
Source(s)	Avis de sécurité IY53894 d'IBM
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

DB2 8.1 Entreprise Edition.

3 Résumé

Une vulnérabilité présente sur le serveur de commande à distance du gestionnaire de base de données DB2 (DB2RCMD.EXE) permet à un utilisateur mal intentionné d'exécuter des commandes arbitraires avec les privilèges du super utilisateur `root`.

4 Description

Une vulnérabilité est présente dans l'exécution de la commande à distance sur le serveur de commande à distance. Lors de la création d'un nouveau processus lancé avec les privilèges du super utilisateur `root` chargé de prendre en charge cette exécution, elle permet à un utilisateur mal intentionné d'exécuter du code arbitraire avec les privilèges du super utilisateur.

5 Solution

Appliquer la mise à jour `FixPack 5` disponible sur le site d'IBM (cf. section documentation).

6 Documentation

– Mise à jour disponible à cette adresse :

<http://www-306.ibm.com/cgi-bin/db2www/data/db2/udb/winos2unix/support/v8fphist.d2w/report>

– Avis de sécurité IY53894 IBM :

http://www-306.ibm.com/cgi-bin/db2www/data/db2/udb/winos2unix/support/aparlib.d2w/display_apar_details?aparno=IY53

Gestion détaillée du document

10 mars 2004 version initiale.