Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 octobre 2005
N° CERTA-2005-AVI-413

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples Vulnérabilités dans IBM DB2

Gestion du document

Référence	CERTA-2005-AVI-413
Titre	Multiples vulnérabilités dans IBM DB2
Date de la première version	19 octobre 2005
Date de la dernière version	–
Source(s)	Bulletins de sécurité IBM du 18 octobre 2005
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 ;
- contournement de la politique de sécurité.

2 Systèmes affectés

IBM DB2 Universal Database 8.x.

3 Résumé

De multiples vulnérabilités dans DB2 permettent à un utilisateur local ou distant mal intentionné de provoquer un déni de service ou de contourner la politique de sécurité du système vulnérable.

4 Description

Six vulnérabilités sont présentes dans DB2 et permettent à un utilisateur local ou distant de provoquer un déni de service ou de contourner la politique de sécurité du système :

- Une erreur dans la mise en œuvre des requêtes SQL (Structured Query Language) contenant des

chaînes de caractères constantes permet à un utilisateur local de provoquer un déni de service par le biais d'une requête malicieusement constituée.
- Une erreur dans la gestion de certains types de tables de hachage provoquant le dépôt de fichiers de journalisation permet à un utilisateur mal intentionné de remplir le système de fichiers induisant potentiellement un déni de service.
- Une erreur dans la gestion des connexions au service `db2agents` se terminant anormalement peut permettre à un utilisateur mal intentionné distant de consommer toutes les ressources processeur du système vulnérable.
- Une erreur dans le système de création d'objets permet à un utilisateur mal intentionné de créer un objet exécutable même s'il ne dispose pas de ce droit.
- Une erreur dans la gestion des requêtes contenant plus de 32000 éléments dans la liste suivant `in` ou ayant trait aux tables `SYSCAT.TABLES` permet à un utilisateur mal intentionné de provoquer un déni de service de l'instance de base courante.
- Une erreur dans le service `db2jd` lors de la connexion de certains clients permet à un utilisateur distant mal intentionné de provoquer un déni de service.

5 Solution

La version 8 FixPak 10 (aussi appelée version 8.2 FixPak 3) corrige ces problèmes :
http://www-1.ibm.com/support/docview.wss?rs=0&uid=swg24010283

6 Documentation

- Site de IBM DB2 :
  http://www-306.ibm.com/software/data/db2
- Liste des bulletins de sécurité IBM DB2 du 18 octobre :
  - Bulletin de sécurité IBM IY70808 :
    http://www-1.ibm.com/support/docview.wss?uid=swg1IY70808
  - Bulletin de sécurité IBM IY70561 :
    http://www-1.ibm.com/support/docview.wss?uid=swg1IY70561
  - Bulletin de sécurité IBM IY71587 :
    http://www-1.ibm.com/support/docview.wss?uid=swg1IY71587
  - Bulletin de sécurité IBM IY71865 :
    http://www-1.ibm.com/support/docview.wss?uid=swg1IY71865
  - Bulletin de sécurité IBM IY70817 :
    http://www-1.ibm.com/support/docview.wss?uid=swg1IY70817
  - Bulletin de sécurité IBM IY72588 :
    http://www-1.ibm.com/support/docview.wss?uid=swg1IY72588
  - Bulletin de sécurité IBM JR21329 :
    http://www-1.ibm.com/support/docview.wss?uid=swg1JR21329

Gestion détaillée du document

19 octobre 2005 version initiale.