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 février 2008
N° CERTA-2008-AVI-048

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Plusieurs vulnérabilités dans IBM DB2 UDB

Gestion du document

Référence	CERTA-2008-AVI-048
Titre	Plusieurs vulnérabilités dans IBM DB2 UDB
Date de la première version	05 février 2008
Date de la dernière version	–
Source(s)	Note de correctif 1256235 d'IBM du 07 janvier 2008
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 ;
- élévation de privilèges.

2 Systèmes affectés

- Les versions d'IBM DB2 UDB version 8 n'ayant pas le correctif Fixpak 16.

3 Résumé

Plusieurs vulnérabilités ont été identifiées dans IBM DB2 UDB. L'exploitation de ces dernières permet, entre autres, à un utilisateur local, d'élever ses privilèges, de provoquer un déni de service ou contourner la politique de sécurité en vigueur.

4 Description

Plusieurs vulnérabilités ont été identifiées dans IBM DB2 UDB. Ainsi, l'outil `DB2PD` permettrait sous certaines conditions à un utilisateur local d'élever ses privilèges à ceux d'administrateur (*root*). Une vulnérabilité similaire se trouve dans l'outil `b2dart` manipulant une commande TPUT. Les conséquences de l'exploitation d'autres vulnérabilités, concernant en particulier le serveur DAS ou la routine `SYSPROC.ADMIN_SP_C` ne sont pas précisées par l'éditeur.

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 swg21256235 du 07 janvier 2008 :
  http://www-1.ibm.com/support/docview.wss?uid=swg21256235
- Corrections apportées par la mise à jour Fixpak 16 pour IBM DB2 UDB Version 8, publiées le 30 janvier 2008 :
  ftp://ftp.software.ibm.com/ps/products/db2/fixes/english-us/aparlist/db2_v82/APARLIST.TXT

Gestion détaillée du document

05 février 2008 version initiale.