

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans la base de données 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-2005-AVI-233>

---

### Gestion du document

Référence	CERTA-2005-AVI-233
Titre	Vulnérabilité dans la base de données DB2
Date de la première version	28 juin 2005
Date de la dernière version	–
Source(s)	APAR Number : IY73104
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

- Perte d'intégrité de la base de données ;
- élévation de privilèges.

## 2 Systèmes affectés

Tous les systèmes DB2 UDB (Universal Database) dans leurs révisions (*service levels*) :

- de la version 8.1.4 à la version 8.1.9 ;
- de la version 8.2.0 à la version 8.2.2.

## 3 Résumé

Une vulnérabilité dans le système DB2 UDB d'IBM permet à un utilisateur doté uniquement de droits en lecture de modifier le contenu de la base de données.

## 4 Description

Une vulnérabilité dans la base de données DB2 permet dans certains cas de contourner la vérification des privilèges. Cette vulnérabilité permet à un utilisateur qui détient le privilège SELECT sur une table, mais qui ne possède par pour autant les privilèges INSERT, UPDATE ou DELETE, de néanmoins insérer, mettre à jour ou détruire des enregistrements dans cette table.

## 5 Contournement provisoire

Un contournement provisoire est de révoquer le privilège SELECT de tous les utilisateurs ou de toutes les applications, sauf pour ceux à qui on a fait confiance au point d'accorder des privilèges supérieurs comme ALTER, CONTROL, DELETE, UPDATE ou INSERT.

## 6 Solution

La problème est corrigé dans les DB2 UDB Version 8 FixPaks 6c, 7b, 8a, 9a ainsi que les versions ultérieures des FixPaks.

## 7 Documentation

- La page décrivant la vulnérabilité chez IBM :  
<http://www-1.ibm.com/support/docview.wss?uid=swg21209727>

## Gestion détaillée du document

28 juin 2005 version initiale.