Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 septembre 2010
N° CERTA-2010-AVI-443-001

**Affaire suivie par :**
CERTA

# AVIS DU CERTA

## Objet : Vulnérabilités dans IBM DB2



## Gestion du document

| | |
|---|---|
| Référence | CERTA-2010-AVI-443-001 |
| Titre | Vulnérabilités dans IBM DB2 |
| Date de la première version | 21 septembre 2010 |
| Date de la dernière version | – |
| Source(s) | Bulletin de sécurité IBM swg2I446455 du 18 septembre 2010 |
| 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

Contournement de la politique de sécurité.

## 2 Systèmes affectés

IBM DB2 version 9.7.

## 3 Résumé

Deux vulnérabilités dans IBM DB2 permettent à un utilisateur malveillant de contourner la politique de sécurité.

## 4 Description

Deux vulnérabilités sont présentes dans IBM DB2 :

– la suppression de droits au groupe `PUBLIC` n'est pas convenablement répercutée sur des fonctions d'accès aux objets de la base de données. Ce défaut permet à un utilisateur malveillant d'utiliser ces fonctions sans droits ;

– si un utilisateur ayant les droits suffisants sur une table donnée exécute une instruction `update` dans une requête SQL compilée et mise en cache, tout utilisateur pourra exécuter cette instruction, même sans droit suffisant.

# 5 Solution

La version 9.7 Fix Pack 3 d'IBM DB2 remédie à ces vulnérabilités.
Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

# 6 Documentation

– Bulletin de sécurité IBM swg2I446455 du 18 septembre 2010 :
http://www-01.ibm.com/support/docview.wss?uid=swg21446455
– Référence CVE CVE-2010-3474 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3474
– Référence CVE CVE-2010-3475 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3475

# Gestion détaillée du document

**20 septembre 2010** version initiale.
**21 septembre 2010** ajout des références CVE.