

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans 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-2005-AVI-077>

---

### Gestion du document

Référence	CERTA-2005-AVI-077
Titre	Multiples vulnérabilités dans IBM DB2
Date de la première version	15 février 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité IBM n°1196289 du 20 janvier 2005
Pièce(s) jointe(s)	

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

## 1 Risque

- Exécution de code arbitraire ;
- atteinte à la confidentialité des données ;
- atteinte à l'intégrité des données ;
- déni de service.

## 2 Systèmes affectés

DB2 Universal Database 8.x.

## 3 Résumé

De nombreuses vulnérabilités découvertes dans IBM DB2 peuvent être exploitées par un utilisateur mal intentionné présent sur le réseau local afin d'exécuter du code arbitraire, d'effectuer un déni de service ou de porter atteinte à la confidentialité ou à l'intégrité des données présentes sur le système vulnérable.

## 4 Description

L'application DB2 d'IBM est une base de données pour les systèmes d'exploitation Linux, UNIX et Windows. Cette application présente de multiples vulnérabilités :

- La version Windows de l'application DB2 d'IBM présente une vulnérabilité dans la méthode utilisée pour gérer les ressources du système. Cette vulnérabilité permet à un utilisateur local mal intentionné d'effectuer un déni de service et de porter atteinte à la confidentialité et à l'intégrité des données ;
- une vulnérabilité découverte dans le traitement des messages réseaux lors d'une connexion à la base de donnée permet à une personne malveillante d'exécuter du code arbitraire ;
- une vulnérabilité affectant certaines fonctions XML-Extender permet à un utilisateur mal intentionné de porter atteinte à la confidentialité et à l'intégrité des données ;
- une vulnérabilité présente lors de la création de certains objets de la base de données permet à un individu malveillant d'exécuter du code arbitraire.

Les vulnérabilités citées ci-dessus ne peuvent être exploitées que si l'option "federated database support" est activée.

Certaines fonctions XML(eXtensible Markup Language) présentent une vulnérabilité qui permet à un utilisateur mal intentionné d'exécuter du code arbitraire sur le système vulnérable.

## 5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs.

## 6 Documentation

- Bulletin de sécurité IBM n° 1196289 du 20 janvier 2005 :  
<http://www-1.ibm.com/support/docview.wss?uid=swg21196289>
- Correctifs fournis par l'éditeur :  
<http://www-306.ibm.com/software/data/db2/udb/support/downloadv8.html>

## Gestion détaillée du document

15 février 2005 version initiale.