



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 14 janvier 2005  
N° CERTA-2005-AVI-015

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilité 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-015>

---

### Gestion du document

Référence	CERTA-2005-AVI-015
Titre	Multiples vulnérabilité dans IBM DB2
Date de la première version	14 janvier 2005
Date de la dernière version	–
Source(s)	Bulletins de sécurité de NGS Research
Pièce(s) jointe(s)	

TAB. 1 – Gestion du document

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

## 1 Risque

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

## 2 Systèmes affectés

- IBM DB2 8.1 ;
- IBM DB2 7.x.

## 3 Résumé

De multiples vulnérabilités découvertes dans l'application DB2 d'IBM permettent à un utilisateur local ou distant d'exécuter du code arbitraire, d'élever ses privilèges ou de porter atteinte à la confidentialité et 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 :

- Une vulnérabilité de type débordement de pile dans `db2fmp` permet à un utilisateur local mal intentionné d'élever ses privilèges. *Remarque : Cette vulnérabilité ne concerne pas le système d'exploitation Microsoft Windows.*
- La bibliothèque `libdb2.so.1` présente une vulnérabilité de type débordement de mémoire. Un utilisateur peut exploiter cette vulnérabilité afin d'élever ses privilèges à l'égal du compte `root` (administrateur).
- Une vulnérabilité de type débordement de pile découverte dans la commande `call` permet à une personne malveillante d'élever ses privilèges à l'égal du compte `root`.
- Une vulnérabilité découverte dans `JDBC Applet Server` de DB2 présente une vulnérabilité de type débordement de pile. Cette vulnérabilité peut être exploitée par une personne mal intentionnée afin d'exécuter du code arbitraire à distance.
- La fonction `SATENCRYPT` présente une vulnérabilité de type débordement de pile qui permet à un utilisateur mal intentionné d'élever ses privilèges à l'égal du compte `root`.
- La version Windows de l'application DB2 d'IBM présente une vulnérabilité permettant à une personne malveillante de porter atteinte à la confidentialité et à l'intégrité des données partagées sur le système vulnérable.
- Une vulnérabilité découverte dans la fonction `to_char()` et dans la fonction `to_date()` permet à un utilisateur mal intentionné d'effectuer un déni de service sur l'application DB2.
- Quatre fonctions XML (`extensible Markup Language`) présentent une vulnérabilité de type débordement de pile. Une personne malveillante peut exploiter ces vulnérabilités afin d'exécuter du code arbitraire et/ou d'élever ses privilèges à l'égal du compte `root`.
- Une seconde vulnérabilité découverte dans les fonctions XML permet à un utilisateur distant mal intentionné de porter atteinte à la confidentialité et à l'intégrité des données.

## 5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. Documentation).

## 6 Documentation

- Bulletin de sécurité NGS Research #NISR05012005A :  
<http://www.nextgenss.com/advisories/db205012005A.txt>
- Bulletin de sécurité NGS Research #NISR05012005B :  
<http://www.nextgenss.com/advisories/db205012005B.txt>
- Bulletin de sécurité NGS Research #NISR05012005C :  
<http://www.nextgenss.com/advisories/db205012005C.txt>
- Bulletin de sécurité NGS Research #NISR05012005D :  
<http://www.nextgenss.com/advisories/db205012005D.txt>
- Bulletin de sécurité NGS Research #NISR05012005E :  
<http://www.nextgenss.com/advisories/db205012005E.txt>
- Bulletin de sécurité NGS Research #NISR05012005F :  
<http://www.nextgenss.com/advisories/db205012005F.txt>
- Bulletin de sécurité NGS Research #NISR05012005G :  
<http://www.nextgenss.com/advisories/db205012005G.txt>
- Bulletin de sécurité NGS Research #NISR05012005H :  
<http://www.nextgenss.com/advisories/db205012005H.txt>
- Bulletin de sécurité NGS Research #NISR05012005I :  
<http://www.nextgenss.com/advisories/db205012005I.txt>
- Mise à jour d'IBM concernant DB2 8.1 :  
<http://www-306.ibm.com/software/data/db2/udb/support/downloadv8.html>
- Mise à jour d'IBM concernant DB2 7.x :  
<http://www-306.ibm.com/software/data/db2/udb/support/downloadv7.html>

# **Gestion détaillée du document**

**14 janvier 2005** version initiale.