



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 04 juin 2010
N° CERTA-2010-AVI-239

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : 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-2010-AVI-239>

Gestion du document

Référence	CERTA-2010-AVI-239
Titre	Vulnérabilités dans IBM DB2
Date de la première version	04 juin 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité IBM swg21432298 du 28 mai 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

- Déni de service à distance ;
- contournement de la politique de sécurité ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

IBM DB2 version 9.7.

3 Résumé

Plusieurs vulnérabilités affectent IBM DB2 et permettent à un utilisateur malveillant de réaliser un déni de service à distance ou de contourner la politique de sécurité.

4 Description

Plusieurs vulnérabilités dans IBM DB2 ont été publiées et corrigées :

- l'agent TIVOLI installé pour DB2 permet à utilisateur distant de provoquer un déni de service ;

- la renégociation des sessions TLS et SSL permet de contourner la politique de sécurité ;
- les droits d'accès accordés peuvent n'être pas pris en considération de manière homogène ;
- des informations pour les administrateurs peuvent être, à tort, publiques.

5 Solution

Le Fix Pack 2 pour IBM DB2 version 9.7 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 swg21432298 du 28 mai 2010 :
<http://www-01.ibm.com/support/docview.wss?uid=swg21432298>
- Document du CERTA CERTA-2009-AVI-482 du 19 mai 2010 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-482/index.html>
- Référence CVE CVE-2009-3555 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3555>
- Référence CVE CVE-2010-0472 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0472>

Gestion détaillée du document

04 juin 2010 version initiale.