Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 avril 2008
N° CERTA-2008-AVI-213

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans IBM DB2

Gestion du document

Référence	CERTA-2008-AVI-213
Titre	Vulnérabilités dans IBM DB2
Date de la première version	17 avril 2008
Date de la dernière version	–
Source(s)	Mises à jour de sécurité IBM du 15 avril 2008
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

- Exécution de code arbitraire ;
- atteinte à l'intégrité des données ;
- élévation de privilèges.

2 Systèmes affectés

- IBM DB2 Universal Database 8.x ;
- IBM DB2 for Linux UNIX and Windows 9.x.

3 Résumé

Deux vulnérabiltés découvertes dans IBM DB2 permettent à un utilisateur local malintentionné de porter atteinte à l'intégrité des données, d'exécuter du code arbitraire avec les droits de l'administrateur.

4 Description

La première vulnérabilité, de type débordement de mémoire, affecte l'application `db2dasrrm` et peut être exploitée en passant à la variable d'environnement `DASPROF` une valeur particulière. L'exploitation de cette vulnérabilité permet à un utilisateur local malintentionné d'exécuter du code arbitraire avec les privilèges de l'administrateur.

La seconde vulnérabilité est causée par un manque de contrôle lors de la création de certains fichiers durant le lancement de l'application `db2dasrrm`. Une personne malveillante peut porter atteinte à l'intégrité des données présentes sur le système au moyen de liens symboliques spécifiquement construits.

5 Solution

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

6 Documentation

- Bulletin de sécurité IBM swg21256235 du 07 janvier 2008 :
  http://www-1.ibm.com/support/docview.wss?uid=swg21256235
- Bulletin de sécurité IBM swg21255572 du 15 janvier 2008 :
  http://www-1.ibm.com/support/docview.wss?uid=swg21255572
- Bulletin de sécurité IBM swg21287889 du 15 avril 2008 :
  http://www-1.ibm.com/support/docview.wss?uid=swg21287889
- Bulletin de sécurité iDefense 688 du 15 avril 2008 :
  http://www.idefense.com/intelligence/vulnerabilities/display.php?id=688
- Bulletin de sécurité iDefense 689 du 15 avril 2008 :
  http://www.idefense.com/intelligence/vulnerabilities/display.php?id=689
- Référence CVE CVE-2007-5664 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5664
- Référence CVE CVE-2007-5758 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5758

Gestion détaillée du document

17 avril 2008 version initiale.