



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 juillet 2004
N° CERTA-2004-AVI-185-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le pilote ODBC de PostgreSQL

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-2004-AVI-185>

Gestion du document

Référence	CERTA-2004-AVI-185-002
Titre	Vulnérabilité dans le pilote ODBC de PostgreSQL
Date de la première version	09 juin 2004
Date de la dernière version	28 juillet 2004
Source(s)	Avis de sécurité Debian DSA-516 du 07 juin 2004
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 ;
- exécution de code arbitraire.

2 Systèmes affectés

Le pilote ODBC `psqlodbc 7.x` du gestionnaire de base de données PostgreSQL.

3 Résumé

Une vulnérabilité présente dans le pilote ODBC (Open DataBase Connectivity) du gestionnaire de base de données PostgreSQL permet à un utilisateur mal intentionné de réaliser un déni de service ou d'exécuter du code arbitraire à distance.

4 Description

Un débordement de mémoire est présent dans la fonction `PGAPI_Connect()` du pilote ODBC. Un utilisateur mal intentionné peut, via une chaîne malicieusement construite, exécuter du code arbitraire sur le système vulnérable.

5 Solution

Appliquer les correctifs (cf. section Documentation).

6 Documentation

- Site Internet PostgreSQL :
<http://www.postgresql.org>
- Avis de sécurité Debian DSA-516 du 07 juin 2004 :
<http://www.debian.org/security/2004/dsa-516>
- Avis de sécurité SUSE SuSE-SA:2004:015 du 09 juin 2004 :
http://www.suse.com/de/security/2004_15_cvs.html
- Avis de sécurité Mandrake MDKSA-2004:072 du 27 juillet 2004 :
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:072>
- Référence CVE CAN-2004-0547 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0547>

Gestion détaillée du document

09 juin 2004 version initiale.

09 juin 2004 ajout du site Internet PostgreSQL et de la référence au bulletin de sécurité de SUSE.

28 juillet 2004 ajout référence au bulletin de sécurité de Mandrake. Ajout référence CVE.