



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 13 septembre 2002  
N° CERTA-2002-AVI-192-001

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités 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-2002-AVI-192>

---

### Gestion du document

Référence	CERTA-2002-AVI-192-001
Titre	Vulnérabilités de PostgreSQL
Date de la première version	27 août 2002
Date de la dernière version	13 septembre 2002
Source(s)	–
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.

## 2 Systèmes affectés

PostgreSQL versions 7.2.1 et antérieures.

## 3 Résumé

Plusieurs vulnérabilités sur PostgreSQL permettent à un utilisateur mal intentionné d'exécuter du code arbitraire.

## 4 Description

PostgreSQL est un gestionnaire de bases de données relationnelles.

Des vulnérabilités de type débordement de mémoire, découvertes dans plusieurs fonctions, permettent à un utilisateur mal intentionné d'exécuter du code arbitraire.

L'utilisateur doit pouvoir se connecter à l'une des bases pour exploiter ces vulnérabilités.

## 5 Contournement provisoire

Pour limiter l'impact des vulnérabilités, vous pouvez :

- bloquer le port sur lequel le serveur PostgreSQL est en écoute (5432/tcp par défaut) au niveau des pare-feux afin d'empêcher l'exploitation de ces vulnérabilités depuis l'Internet ;
- ne pas accepter les connexions non authentifiées (*trust authentication*) à la base de données.  
Editez pour cela le fichier *pg\_hba.conf*.

## 6 Solution

La version 7.2.2 corrige ces vulnérabilités.

## 7 Documentation

Avis de PostgreSQL :

<http://www.fr.postgresql.org/news.html>

Avis de sécurité Debian DSA 165-1 :

<http://www.debian.org/security/2002/DSA-165>

## Gestion détaillée du document

**27 août 2002** version initiale ;

**13 septembre 2002** première révision : ajout de l'avis Debian.