



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 26 mars 2007
N° CERTA-2007-AVI-069-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités sous 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-2007-AVI-069>

Gestion du document

Référence	CERTA-2007-AVI-069-002
Titre	Multiples vulnérabilités sous PostgreSQL
Date de la première version	06 février 2007
Date de la dernière version	26 mars 2007
Source(s)	Bulletin de sécurité PostgreSQL
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 ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- PostgreSQL 7.3 ;
- PostgreSQL 7.4 ;
- PostgreSQL 8.0 ;
- PostgreSQL 8.1 ;
- PostgreSQL 8.2.

3 Résumé

Plusieurs vulnérabilités de PostgreSQL permettent à une personne malveillante de réaliser un déni de service et de contourner la politique de sécurité.

4 Description

Deux vulnérabilités ont été identifiées dans PostgreSQL.

La première (CVE-2007-0555) permet à un utilisateur malintentionné, en supprimant les informations renvoyées par certaines fonctions de contrôle, de réaliser un déni de service et d'accéder à des données protégées.

La seconde (CVE-2007-0556) permet à un utilisateur malintentionné, en changeant le type de données d'une colonne, de réaliser un déni de service et d'accéder à des données protégées.

5 Solution

Les versions 8.2.2, 8.1.7, 8.0.11, 7.4.16 et 7.3.13 de PostgreSQL corrigent les problèmes. Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité PostgreSQL :
<http://www.postgresql.org/support/security>
- Bulletin de sécurité Debian DSA-1261 du 15 mars 2007 :
<http://www.us.debian.org/security/2007/dsa-1261>
- Bulletin de sécurité Gentoo GLSA-200703-15 du 16 mars 2007 :
<http://www.gentoo.org/security/en/glsa/glsa-200703-15.xml>
- Bulletin de sécurité Mandriva MDKSA-2007:037 du 06 février 2007 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2007:037>
- Bulletin de sécurité Red Hat RHSA-2007:0064 du 07 février 2007 :
<http://rhn.redhat.com/errata/RHSA-2007-0064.html>
- Bulletin de sécurité Ubuntu USN-417-1 du 05 février 2007 :
<http://www.ubuntu.com/usn/usn-417-1>
- Bulletin de sécurité Ubuntu USN-417-2 du 06 février 2007 :
<http://www.ubuntu.com/usn/usn-417-2>
- Bulletin de sécurité Ubuntu USN-417-3 du 09 février 2007 :
<http://www.ubuntu.com/usn/usn-417-3>
- Bulletin de sécurité Avaya ASA-2007-117 du 19 mars 2007 :
<http://www.support.avaya.com/elmodocs2/security/ASA-2007-117.htm>
- Référence CVE CVE-2007-0555 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0555>
- Référence CVE CVE-2007-0556 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0556>
- Bulletin de sécurité Sun Solaris #102825 du 27 février 2007 :
<http://sunsolve.sun.com/search/document.do?assetkey=1-102825-1>

Gestion détaillée du document

06 février 2007 version initiale.

01 mars 2007 ajout de la référence au bulletin de sécurité Sun Solaris.

26 mars 2007 ajout des références aux bulletins de sécurité Debian, Gentoo, Mandriva, Red Hat, Ubuntu et Avaya.