Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 août 2006
N° CERTA-2006-AVI-216-004

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans PostgreSQL

Gestion du document

Référence	CERTA-2006-AVI-216-004
Titre	Vulnérabilités dans PostgreSQL
Date de la première version	24 mai 2006
Date de la dernière version	21 août 2006
Source(s)	Bulletin de sécurité postgreSQL du 22 mai 2006
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

- Contournement de la politique de sécurité ;
- atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- La version PostgreSQL 7.3.14 et les versions 7.3.x antérieures ;
- la version PostgreSQL 7.4.12 et les versions 7.4.x antérieures ;
- la version PostgreSQL 8.0.7 et les versions 8.0.x antérieures ;
- la version PostgreSQL 8.1.3 et les versions 8.1.x antérieures.

3 Résumé

Deux vulnérabilités ont été identifiées dans PostgreSQL. Elles peuvent être utilisées par une personne malveillante pour injecter des requêtes SQL, afin d'accéder ou modifier les données inclues dans la base, et ainsi contourner la politique de sécurité.

4 Description

PostgreSQL est un système de gestion de bases de données (DBMS). Deux vulnérabilités ont été identifiées dans certaines versions du serveur. Il ne contrôle pas correctement certains caractères d'échappement, tels que le guillemet `'`. Un utilisateur malveillant peut profiter de ce problème pour injecter, soit directement, soit par le biais d'une application tierce, des requêtes SQL arbitraires. La politique de sécurité est alors contournée.

5 Solution

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

6 Documentation

- Bulletin de sécurité PostgreSQL du 22 mai 2006 :
  http://www.postgresql.org/docs/techdocs.50
- Page de mise à jour PostgreSQL :
  http://www.postgresql.org/download
- Bulletin de sécurité RedHat du 26 mai 2006 :
  http://rhn.redhat.com/errata/RHSA-2006-0526.html
- Bulletin de sécurité Debian DSA-1087 du 03 juin 2006 :
  http://www.debian.org/security/2006/dsa-1087
- Bulletin de sécurité Mandriva MDKSA-2006:098 du 07 juin 2006 :
  http://www.mandriva.com/security/advisories?name=MDKSA-2006:098
- Bulletin de sécurité FreeBSD :
  http://www.vuxml.org/freebsd/pkg-ja-postgresql.html
- Référence CVE CVE-2006-2313 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2313
- Référence CVE CVE-2006-2314 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2314

Gestion détaillée du document

24 mai 2006 version initiale ;
26 mai 2006 ajout de la référence au bulletin de sécurité RedHat.
06 juin 2006 ajout de la référence au bulletin de sécurité Debian.
08 juin 2006 ajout de la référence au bulletin de sécurité Mandriva.
21 août 2006 ajout de la référence au bulletin de sécurité FreeBSD.