

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans 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-2008-AVI-005>

Gestion du document

| | |
|-----------------------------|--|
| Référence | CERTA-2008-AVI-005 |
| Titre | Vulnérabilités dans PostgreSQL |
| Date de la première version | 08 janvier 2008 |
| Date de la dernière version | – |
| Source(s) | Bulletin de sécurité PostgreSQL du 06 janvier 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

- Déni de service ;
- élévation de privilèges.

2 Systèmes affectés

PostgreSQL versions 7.3, 7.4, 8.0, 8.1 et 8.2.

3 Résumé

Des vulnérabilités dans *PostgreSQL* permettent de réaliser un déni de service ou une élévation de privilèges.

4 Description

Plusieurs vulnérabilités ont été découvertes dans *PostgreSQL* :

- une des fonctionnalités de *PostgreSQL* permet de créer une indexation des résultats de fonctions définies par l'utilisateur. Des vulnérabilités dans les fonctions d'indexation permettent d'élever les privilèges de l'utilisateur (CVE-2007-6600) ;

- des problèmes ont été découverts dans les bibliothèques permettant le traitement des expressions régulières par *PostgreSQL*. Un utilisateur malintentionné peut, par le biais d'expressions régulières spécifiques, réaliser un déni de service (CVE-2007-4769, CVE-2007-4772 et CVE-2007-6067) ;
- une vulnérabilité dans les fonctions `DBLink` permet l'élévation des privilèges (CVE-2007-6601).

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 06 janvier 2008 :
<http://www.postgresql.org/about/news.905>
- Mises à jour de sécurité Debian DSA-1460 :
<http://www.debian.org/security/2008/dsa-1460>
- Mises à jour de sécurité Red Hat RHSA-2008-0038 et RHSA-2008-0039 :
<http://www.redhat.com/support/errata/RHSA-2008-0038.html>
<http://www.redhat.com/support/errata/RHSA-2008-0039.html>
- Mises à jour de sécurité Mandriva MDVSA-2008:004 :
<http://www.mandriva.com/security/advisories?name=MDVSA-2008:004>
- Référence CVE CVE-2007-4769 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4769>
- Référence CVE CVE-2007-4772 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4772>
- Référence CVE CVE-2007-6067 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6067>
- Référence CVE CVE-2007-6600 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6600>
- Référence CVE CVE-2007-6601 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6601>

Gestion détaillée du document

08 janvier 2008 version initiale.