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 décembre 2004
N° CERTA-2004-AVI-352-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité 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-2004-AVI-352

Gestion du document

Référence	CERTA-2004-AVI-352-002
Titre	Vulnérabilité dans PostgreSQL
Date de la première version	21 octobre 2004
Date de la dernière version	21 décembre 2004
Source(s)	Bulletin de sécurité Gentoo GLSA-200410-16 du 18 octobre 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

Atteinte à l'intégrité des données.

2 Systèmes affectés

PostgreSQL 7.4.5-r1 et versions antérieures.

3 Résumé

Une vulnérabilité découverte dans PostgreSQL permet à un utilisateur local, mal intentionné, de porter atteinte à l'intégrité des données présentes sur le système.

4 Description

PostgreSQL est un outil de base de données Open Source. Une vulnérabilité présente dans le script `make_oidjoins_check` permet à un utilisateur mal intentionné, ayant un accès local au système, de forcer la modification de fichiers avec les droits d'un autre utilisateur au moyen de liens symboliques habilement constitués.

5 Solution

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

6 Documentation

- Annonce de sécurité PostgreSQL du 23 octobre 2004 :
  http://www.postgresql.org/news/234.html
- Bulletin de sécurité Gentoo GLSA-200410-16 du 18 octobre 2004 :
  http://www.gentoo.org/security/en/glsa/glsa-200410-16.xml
- Bulletin de sécurité Debian DSA-577 du 29 octobre 2004 :
  http://www.debian.org/security/2004/dsa-577
- Bulletin de sécurité Mandrake MDKSA-2004:149 du 13 décembre 2004 :
  http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:149
- Bulletin de sécurité FreeBSD pour postgresql-contrib du 06 novembre 2004 :
  http://www.vuxml.org/freebsd/
- Bulletin de sécurité Red Hat RHSA-2004:489 du 20 décembre 2004 :
  http://rhn.redhat.com/errata/RHSA-2004-489.html
- Référence CVE CAN-2004-0977 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0977

Gestion détaillée du document

21 octobre 2004 version initiale.

16 décembre 2004 Mention de la réference CVE et de l'annonce PostgreSQL. Ajout références aux bulletins de sécurité de Debian, Mandrake et FreeBSD.

21 décembre 2004 ajout référence au bulletin de sécurité de Red Hat.