Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 octobre 2009
N° CERTA-2009-AVI-380-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans PostgreSQL

Gestion du document

Référence	CERTA-2009-AVI-380-001
Titre	Multiples vulnérabilités dans PostgreSQL
Date de la première version	11 septembre 2009
Date de la dernière version	12 octobre 2009
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 à distance ;
- contournement de la politique de sécurité ;
- élévation de privilèges.

2 Systèmes affectés

- PostgreSQL 7.4.26 ;
- PostgreSQL 8.x.

3 Résumé

Plusieurs vulnérabilités dans `PostgreSQL` permettent à une personne malintentionnée de provoquer un déni de service à distance, de contourner la politique de sécurité ou d'élever ses privilèges sur le système.

4 Description

Plusieurs vulnérabilités ont été découvertes dans `PostgreSQL` :

- une erreur dans la fonction *RESET SESSION AUTHORIZATION* permet à une personne malintentionnée d'élever ses privilèges sur le système ;
- une erreur dans la liaison avec un annuaire *LDAP* permet dans certaines conditions de contourner le mécanisme d'authentification ;
- une erreur dans la gestion du rechargement de la librairie *$libdir/plugins* permet de provoquer un déni de service.

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 :
  http://www.postgresql.org/support/security.html
- Bulletin de sécurité Debian DSA-1900 du 02 octobre 2009 :
  http://www.debian.org/security/2009/dsa-1900
- Bulletin de sécurité RedHat RHSA-2009:1484 du 07 octobre 2009 :
  http://rhn.redhat.com/errata/RHSA-2009-1484.html
- Bulletin de sécurité RedHat RHSA-2009:1485 du 10 octobre 2009 :
  http://rhn.redhat.com/errata/RHSA-2009-1485.html
- Référence CVE CVE-2009-3229 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3229
- Référence CVE CVE-2009-3230 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3230
- Référence CVE CVE-2009-3231 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3231

Gestion détaillée du document

11 septembre 2009 version initiale.
12 octobre 2009 ajout des références aux bulletins de sécurité Debian, et RedHat et des références CVE.