Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 07 janvier 2010
N° CERTA-2009-AVI-546-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans PostgreSQL

Gestion du document

Référence	CERTA-2009-AVI-546-001
Titre	Vulnérabilités dans PostgreSQL
Date de la première version	16 décembre 2009
Date de la dernière version	07 janvier 2010
Source(s)	Bulletin de version PostgreSQL du 14 décembre 2009
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

- Élévation de privilèges ;
- contournement de la politique de sécurité.

2 Systèmes affectés

Toutes les versions de PostgreSQL.

3 Résumé

Plusieurs vulnérabilités affectent PostgreSQL et permettent à un utilisateur malveillant de contourner la politique de sécurité ou d'élever ses privilèges.

4 Description

Plusieurs vulnérabilités sont présentes dans PostgreSQL :

- (CVE-2009-4034) la validation des certificats dans lesquels le nom ou le nom alternatif comportent un caractère nul permet à un utilisateur malveillant de contourner la politique de sécurité ;

– (CVE-2009-4136) dans certaines conditions, le changement de l'état d'une session permet à un utilisateur malveillant d'élever ses privilèges.

5 Solution

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

6 Documentation

– Site de téléchargement du projet PostgreSQL :
http://www.postgresql.org/
– Bulletin de version PostgreSQL du 14 décembre 2009 :
http://www.postgresql.org/about/news.1170
– Référence CVE CVE-2009-4034 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4034
– Référence CVE CVE-2009-4136 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4136
– Bulletin de sécurité Ubuntu USN-876-1 du 03 janvier 2010 :
http://www.ubuntu.com/usn/USN-876-1
– Bulletin de sécurité de Debian DSA-1964 du 31 décembre 2009 :
http://www.us.debian.org/security/2009/dsa-1964

Gestion détaillée du document

16 décembre 2009 version initiale.
07 janvier 2010 Ajout des références aux bulletins de sécurité Ubuntu et Debian.