Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 février 2012
N° CERTA-2012-AVI-101

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans PostgreSQL

Gestion du document

Référence	CERTA-2012-AVI-101
Titre	Multiples vulnérabilités dans PostgreSQL
Date de la première version	28 février 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité PostgreSQL du 27 février 2012
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

- Exécution de code arbitraire à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- *PostgreSQL* versions 9.1.3 et antérieures ;
- *PostgreSQL* versions 9.0.7 et antérieures ;
- *PostgreSQL* versions 8.4.11 et antérieures ;
- *PostgreSQL* versions 8.3.18 et antérieures.

3 Résumé

De multiples vulnérabilités ont été corrigées dans *PostgreSQL*, permettant notamment d'exécuter du code arbitraire à distance et de contourner la politique de sécurité.

4 Description

De multiples vulnérabilités ont été découvertes dans *PostgreSQL* :

- les restrictions d'exécution des fonctions peuvent être contournées par les utilisateurs sous certaines conditions (CVE-2012-0866) ;
- lorsque des certificats SSL sont utilisés, il est possible d'usurper un nom de machine si celui-ci fait exactement 32 caractères (CVE-2012-0867) ;
- il est possible d'exécuter des commandes SQL via des noms d'objet spécifiques (CVE-2012-0868).

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 27 février 2012 :
  http://www.postgresql.org/about/news/1377/
- Référence CVE CVE-2012-0866 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0866
- Référence CVE CVE-2012-0867 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0867
- Référence CVE CVE-2012-0868 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0868

Gestion détaillée du document

28 février 2012 version initiale.