Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 mars 2002
N° CERTA-2002-AVI-055

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Contournement de l'autentification pam-pgsql

Gestion du document

Référence	CERTA-2002-AVI-055
Titre	Contournement de l'autentification pam-pgsql
Date de la première version	19 mars 2002
Date de la dernière version	–
Source(s)	Avis FreeBSD-SA-02:14 Avis RUS-CERT
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

Manipulation d'une base de données contenants des noms et des mots de passe.

2 Systèmes affectés

Toutes les versions de `pam-pgsql port` sur FreeBSD antérieures à la version 0.5.2 sur FreeBSD.
L'usage de `pam-pgsql` peut être associé aux outils `login` et `sshd`.

3 Résumé

Une vulnérabilité dans un module d'authentification peut contribuer à contourner les mots de passe.

4 Description

PAM (*Pluggable Authentification Modules*) est un système d'authentification utilisé sur les systèmes Unix. Ce système modulaire permet de développer des applications comme `login` qui nécessitent une authentification sans avoir à se préoccuper du mécanisme d'authentification qui sera mis en œuvre.

Un des modules d'authentification, pam-pgsql repose sur une base de données PostgresSQL.

Les versions vulnérables de pam-pgsql permettent à un utilisateur local ou distant, pouvant mettre en œuvre l'authentification pam-pgsql, de pouvoir soumettre n'importe quelle requête SQL à la base de données contenant les noms et mots de passe.

Les versions antérieures à 0.3, permettent de surcroît à un utilisateur de contourner le mécanisme de vérification des mots de passe.

5 Contournement provisoire

Désinstaller pam-pgsql si on ne s'en sert pas.

6 Solution

Charger un nouveau squelette du portage de pam-pgsql sur
http://www.freebsd.org/ports , utilisez pour reconstruire le portage sur FreeBSD.

7 Documentation

– ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-02:14.pam-pgsql.asc

Gestion détaillée du document

19 mars 2002 version initiale.