Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 janvier 2006
N° CERTA-2006-AVI-020-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans mod_auth_pgsql pour Apache

Gestion du document

Référence	CERTA-2006-AVI-020-001
Titre	Vulnérabilité dans mod_auth_pgsql pour Apache
Date de la première version	11 janvier 2006
Date de la dernière version	16 janvier 2006
Source(s)	Bulletin de sécurité iDefense du 09 janvier 2006
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.

2 Systèmes affectés

`mod_auth_pgsql` version 2.0.2b1 pour Apache 2.x. D'autres versions antérieures peuvent être affectées.

3 Résumé

Une vulnérabilité dans le module `mod_auth_pgsql` pour Apache 2.x permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

4 Description

`mod_auth_pgsql` permet la mise en œuvre dans Apache de l'authentification à partir d'une base de données PostgreSQL. Un manque de contrôle du nom d'utilisateur (username) fourni lors de l'authentification permet à un utilisateur distant mal intentionné d'exécuter du code arbitraire à distance par le biais d'un nom d'utilisateur malicieusement constitué.

5 Solution

La version 2.0.3 de `mod_auth_pgsql` corrige ce problème (voir Documentation).

6 Documentation

- Version 2.0.3 de `mod_auth_pgsql` :
  http://www.giuseppetanzilli.it/mod_auth_pgsql2/dist/
- Bulletin de sécurité iDefense du 09 janvier 2006 :
  http://www.idefense.com/application/poi/display?id=367
- Bulletin de sécurité Red Hat RHSA-2006:0164 du 05 janvier 2006 :
  http://rhn.redhat.com/errata/RHSA-2006-0164.html
- Bulletin de sécurité Mandriva MDKSA-2006:009 du 06 janvier 2006 :
  http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:009
- Bulletin de sécurité Debian DSA-935 du 10 janvier 2006 :
  http://www.debian.org/security/2006/dsa-935
- Bulletin de sécurité Gentoo GLSA 200601-05 du 10 janvier 2006 :
  http://www.gentoo.org/security/en/glsa/glsa-200601-05.xml
- Référence CVE CAN-2005-3656 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3656

Gestion détaillée du document

11 janvier 2006 version initiale.
16 janvier 2006 ajout des références aux bulletins de sécurité Mandriva et Gentoo.