



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 29 décembre 2008
N° CERTA-2008-AVI-613

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de phpPgAdmin

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-613>

Gestion du document

Référence	CERTA-2008-AVI-613
Titre	Vulnérabilité de phpPgAdmin
Date de la première version	29 décembre 2008
Date de la dernière version	–
Source(s)	CVE-2008-5587
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

Contournement de la politique de sécurité.

2 Systèmes affectés

phpPgAdmin, version 4.2.1 et versions antérieures.

3 Résumé

Une vulnérabilité de *phpPgAdmin* permet à un utilisateur malveillant de contourner la politique de sécurité.

4 Description

phpPgAdmin est une interface web d'administration de bases de données *PostgreSQL*.

La validation des données entrées par l'utilisateur est insuffisante. Cette vulnérabilité permet à un utilisateur malveillant de lire des fichiers et d'exécuter des scripts locaux avec les droits du processus du serveur web.

5 Solution

La version 4.2.2 résoud le problème.

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

6 Documentation

- Site de téléchargement du projet phpPgAdmin :
<http://phpPgAdmin.sourceforge.net>
- Bulletin de sécurité Debian DSA 1693 du 27 décembre 2008 :
<http://www.debian.org/security/2008/dsa-1693>
- Bulletin de sécurité Fedora FEDORA-2008-11576 du 21 décembre 2008 :
<https://www.redhat.com/archives/fedora-package-announce/2008-December/msg01109.html>
- Bulletin de sécurité Fedora FEDORA-2008-11602 du 21 décembre 2008 :
<https://www.redhat.com/archives/fedora-package-announce/2008-December/msg01025.html>
- Référence CVE CVE-2008-5587 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5587>

Gestion détaillée du document

29 décembre 2008 version initiale.