Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 23 juillet 2002
N° CERTA-2002-AVI-154

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités sur PHP

Gestion du document

Référence	CERTA-2002-AVI-154
Titre	Vulnérabilités sur PHP
Date de la première version	23 juillet 2002
Date de la dernière version	–
Source(s)	Avis CA-2002-21 du CERT/CC
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

- Déni de service ;
- élévation de privilèges ;
- exécution de code arbitraire.

2 Systèmes affectés

PHP versions 4.2.0 et 4.2.1.

3 Résumé

Plusieurs débordements de mémoire présents sur PHP permettent à un utilisateur mal intentionné de réaliser un déni de service ou d'exécuter du code arbitraire sur le système.

4 Description

Plusieurs vulnérabilités, de type « débordement de mémoire », sont présentes dans la fonction `php_mime_split`. Les vulnérabilités sur cette fonction qui est appelée lors de l'envoi des requêtes `multipart/form-data POST` peuvent permettre à un utilisateur mal intentionné de réaliser un déni de service ou d'exécuter du code arbitraire sur le système.

5 Contournement provisoire

Interdire les requêtes `POST` sur le serveur web.

6 Solution

Appliquer les correctifs correspondant à votre éditeur ou installer la version 4.2.2 (cf site PHP, section documentation).

7 Documentation

- Version 4.2.2 de PHP disponible sur :
  http://www.php.net/downloads.php
- Avis de sécurité CA-2002-21 du CERT/CC :
  http://www.cert.org/advisories/CA-2002-21.html
- Avis de sécurité de e-matters :
  http://security.e-matters.de/advisories/012002.html

Gestion détaillée du document

23 juillet 2002 version initiale.