



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 février 2003
N° CERTA-2003-AVI-025-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans PHP

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-2003-AVI-025>

Gestion du document

Référence	CERTA-2003-AVI-025-001
Titre	Vulnérabilité dans PHP
Date de la première version	18 février 2003
Date de la dernière version	21 février 2003
Source(s)	Avis de sécurité du PHP Group du 17/02/2003
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

Toutes les versions de PHP antérieures ou égales à la version 4.3.0.

3 Résumé

Une vulnérabilité dans PHP permet à un utilisateur mal intentionné de contourner la politique de sécurité (accès en lecture à des fichiers non autorisés).

4 Description

PHP (Personal Home Page) est un langage de script très largement utilisé dans le domaine des développements internet. Une vulnérabilité dans PHP CGI SAPI permet à un utilisateur mal intentionné d'avoir accès à n'importe quel fichier accessible en lecture par l'utilisateur sous lequel est lancé le serveur web, à la condition que le serveur web utilise le module CGI.

5 Solution

La version 4.3.1 de PHP corrige cette vulnérabilité. Cette version est disponible à l'adresse suivante :
<http://www.php.net/downloads.php>

La version 4.3.0 corrige une vulnérabilité dans la fonction `wordwrap()` sujette à un débordement de mémoire. Les versions affectées par ce débordement de tampon sont les versions de PHP ultérieures à la version 4.1.2 et antérieures à la version 4.3.0.

6 Documentation

Avis de sécurité du PHP Group du 17 février 2003 :
http://www.php.net/release_4_3_1.php

Gestion détaillée du document

18 février 2003 version initiale.

21 février 2003 ajout d'une référence à une vulnérabilité (fonction `wordwrap()`) dans PHP version ultérieure à la version 4.1.2 et antérieure à la version 4.3.0.