



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 février 2002
N° CERTA-2002-AVI-047

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités de 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-2002-AVI-047>

Gestion du document

Référence	CERTA-2002-AVI-047
Titre	Vulnérabilités de PHP
Date de la première version	28 février 2002
Date de la dernière version	–
Source(s)	Avis de sécurité CA-2002-05 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

Exécution d'un code arbitraire à distance.

2 Systèmes affectés

- PHP de la version 3.10 à la version 3.18.
- PHP de la version 4.0.1 à la version 4.1.1

3 Résumé

Plusieurs vulnérabilités de type « débordement de mémoire » permettent à un utilisateur mal intentionné d'exécuter un code arbitraire à distance.

4 Description

PHP est un langage permettant la création de pages Web dynamiques.

Plusieurs débordements de mémoire présents dans la fonction `php_mime_split` (fonction servant à traiter les requêtes HTTP de type «POST multiple-part») permettent à un utilisateur mal intentionné l'exécution d'un code arbitraire à distance.

5 Contournement provisoire

Désactiver la fonction `upload` (`file_upload = off`) dans le fichier `php.ini`.

6 Solution

Installer la version 4.1.2 de PHP disponible sur <http://www.php.net> ou appliquer le correctif de la version concernée.

7 Documentation

Avis de sécurité CA-2002-05 du CERT/CC :
<http://www.cert.org/advisories/CA-2002-05.html>

Gestion détaillée du document

28 février 2002 version initiale.