

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités 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-2006-AVI-171>

Gestion du document

Référence	CERTA-2006-AVI-171
Titre	Multiples vulnérabilités dans PHP
Date de la première version	27 avril 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Mandriva MDKSA-2006:074 du 24 avril 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

- Contournement de la politique de sécurité ;
- Attaque de type Cross Site Scripting.

2 Systèmes affectés

- PHP 4.x.x ;
- PHP 5.x.x.

3 Résumé

Plusieurs vulnérabilités découvertes dans PHP permettent à un utilisateur distant mal intentionnée contourner la politique de sécurité et/ou de réaliser des attaques de type injection de code indirecte (Cross Site Scripting).

4 Description

PHP est un langage de script permettant la réalisation de pages web dynamiques.

- une vulnérabilité dans la fonction `phpinfo()` peut être exploitée par un utilisateur mal intentionné, au moyen d'argument long et astucieusement formé, afin de placer du code arbitraire sur le serveur vulnérable qui sera exécuté depuis le poste d'un internaute.
- deux vulnérabilités dans les fonctions `tempnam()` et `copy()` permettent à un individu distant mal intentionné de contourner la politique de sécurité.

5 Solution

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

6 Documentation

- Bulletin de sécurité Mandriva MDKSA-2006:074 du 24 avril 2006 :
<http://wwwnew.mandriva.com/security/advisories?name=MDKSA-2006:074>
- Référence CVE CAN-2006-0996 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-0996>
- Référence CVE CAN-2006-1494 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-1494>
- Référence CVE CAN-2006-1608 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-1608>

Gestion détaillée du document

27 avril 2006 version initiale.