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 novembre 2005
N° CERTA-2005-AVI-468

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans phpSysInfo

Dernière version de ce document : http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-468

Gestion du document

Référence	CERTA-2005-AVI-468
Titre	Vulnérabilité dans phpSysInfo
Date de la première version	23 novembre 2005
Date de la dernière version	–
Source(s)	Mise à jour de sécurité pour phpSysInfo en version 2.4.1
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 de code arbitraire à distance ;
- atteinte à la confidentialité des données ;
- atteinte à l'intégrité des données ;
- `cross site scripting`.

2 Systèmes affectés

- phpSysInfo 1.x ;
- phpSysInfo 2.x.

3 Résumé

Une vulnérabilité dans phpSysInfo permet à un utilisateur mal intentionné de porter atteinte à l'intégrité des donnéees présentes sur le serveur vulnérable pour ensuite exécuter du code arbitraire à distance sur les postes clients.

4 Description

phpSysInfo est un programme en langage `php` qui retourne graphiquement des informations sur système.

Une vulnérabilité dans l'émulation `register_globals` permet à un utilisateur mal intentionné de porter atteinte à l'intégrité des donnéees présentes sur le serveur afin de s'en servir pour exécuter du code arbitraire à distance sur les postes clients.

5 Solution

Appliquer la mise à jour de sécurité phpSysInfo en passant à la version 2.4.1 disponible à l'adresse suivante : http://sourceforge.net/project/showfiles.php?group_id=15

6 Documentation

- Mise à jour de sécurité pour phpSysInfo en version 2.4.1 du 20 novembre 2005 : http://sourceforge.net/project/showfiles.php?group_id=15
- Bulletin de sécurité Hardened-php #22/2005 du 13 novembre 2005 : http://www.hardened-php.net/advisory_222005.81.html
- Référence CVE CAN-2005-3347 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3347
- Référence CVE CAN-2005-3349 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3348

Gestion détaillée du document

23 novembre 2005 version initiale.