



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 05 janvier 2009
N° CERTA-2008-AVI-593-001

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-2008-AVI-593>

Gestion du document

Référence	CERTA-2008-AVI-593-001
Titre	Vulnérabilité dans PHP
Date de la première version	11 décembre 2008
Date de la dernière version	05 janvier 2009
Source(s)	Changement de version PHP 5.2.8 du 08 décembre 2008
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

– PHP version 5.2.7.

3 Résumé

La version 5.2.7 de PHP récemment publiée présente une régression de fonctionnalité des `magic_quotes` pouvant permettre de contourner la politique de sécurité mise en place.

4 Description

La version 5.2.7 de PHP récemment publiée présente une régression de fonctionnalité des `magic_quotes`. Une extension de filtrage (`ext/filter`) change la valeur de `magic_quotes_gpc` à "off", rendant le site potentiellement vulnérable à certaines classes d'attaques.

5 Solution

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

6 Documentation

- Note de changement PHP 5.2.8 du 08 décembre 2008 :
<http://www.php.net/archive/2008#id2008-12-08-01>
- Signalement d'erreur PHP par S. Esser :
<http://www.suspekt.org/2008/12/07/php-527-beware-magic-quotes-gpc-broken/>
- Avis JVN JVNDB-2008-000084 du 19 décembre 2008 :
<http://jvndb.jvn.jp/en/contents/2008/JVNDB-2008-000084.html>
- Référence CVE CVE-2008-5814 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5814>

Gestion détaillée du document

11 décembre 2008 version initiale.

05 janvier 2009 ajout d'une référence CVE associée.