



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 mars 2007
N° CERTA-2007-AVI-117

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de PMB

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-2007-AVI-117>

Gestion du document

Référence	CERTA-2007-AVI-117
Titre	Vulnérabilité de PMB
Date de la première version	12 mars 2007
Date de la dernière version	–
Source(s)	Interne
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.

2 Systèmes affectés

PMB version 3.0.14 et antérieures.

3 Résumé

Une vulnérabilité sur trois variables PHP permet à un utilisateur malveillant d'exécuter du code arbitraire à distance.

4 Description

PMB ou *PhpMyBibli* est un logiciel libre de gestion de bibliothèque développé en langage PHP et prenant en compte le format UNIMARC.

Pour trois variables PHP, la vérification de la valeur affectée n'est pas assez restrictive. Cela peut être exploité par un utilisateur malveillant pour exécuter du code arbitraire à distance.

La vulnérabilité est massivement exploitée par un code malveillant disponible sur l'Internet..

Lorsque la variable `register_globals` du fichier de paramétrage `php.ini` est positionnée à la valeur `off`, la vulnérabilité n'est pas exploitable.

5 Solution

La version 3.0.15 corrige la vulnérabilité. Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Page de téléchargement de l'éditeur :
<http://www.sigb.net/download.php>

Gestion détaillée du document

12 mars 2007 version initiale.