Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 09 septembre 2003
N° CERTA-2003-ALE-003

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Exploitation massive de la vulnérabilité « include PHP »

Gestion du document

Référence	CERTA-2003-ALE-003
Titre	Exploitation massive de la vulnérabilité « include PHP »
Date de la première version	09 septembre 2003
Date de la dernière version	–
Source(s)	
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

- Défiguration de site WEB ;
- divulgation d'informations sensibles ;
- compromission à distance du système.

2 Systèmes affectés

Les systèmes potentiellement affectés sont les applications WEB écrites en PHP qui utilisent la directive `include` sans précaution.

3 Résumé

Par une URL astucieusement constituée visant un script PHP vulnérable tournant sur un serveur WEB, un individu mal intentionné peut prendre connaissance de documents sensibles présents sur le serveur ou faire exécuter au serveur n'importe quelle commande avec les droits du serveur HTTP.

Cette vulnérabilité est actuellement largement utilisée.

4 Description

PHP est un langage destiné essentiellement à la réalisation de « pages HTML dynamiques » sur un serveur WEB.

Une fonctionnalité de ce langage de programmation permet de construire des sites WEB en répartissant le code ou le texte dans différents fichiers qui seront inclus au moment de la visualisation de la page en utilisant la directive `<? include $quelquechose ?>`.

Un problème de sécurité se pose dès lors que deux conditions sont réunies :

1° un internaute peut affecter précisément le contenu de la variable `$quelquechose` avec une URL habilement constituée ;

2° l'application PHP ne filtre pas avec la plus grande rigueur le contenu de cette variable afin de s'assurer qu'elle ne fait pas référence à une page distante (accessible par exemple au travers des protocoles `http://` ou `ftp://`, ce qui entraîne le risque d'exécution de code arbitraire) ou une page locale (ce qui entraîne un risque de divulgation d'informations sensibles).

Par ailleurs, n'importe quelle variable d'une page dynamique peut être redéfinie par une URL astucieusement construite.

On assiste actuellement à une exploitation massive de cette vulnérabilité dans le but de défigurer le contenu de serveurs WEB.

5 Solution

La seule solution fiable est de ne *jamais* utiliser des lignes de code du type `<? include $quelquechose ?>`, dès lors que la variable `$quelquechose` dépend des champs de la requête HTTP `GET` ou `POST`.

Au même titre que les vulnérabilités de type « injection SQL » ou « cross site scripting », le seul moyen fiable de vérifier que l'on n'est pas vulnérable est de procéder à l'analyse en profondeur du code PHP de ses applications.

Le guide donné dans la documentation précise les règles de programmation à appliquer sur un développement PHP pour se prémunir contre ce type d'attaque.

6 Documentation

– http://www.dwheeler.com/secure-programs/Secure-Programs-HOWTO.html#PHP
Ce document précise quelques bonnes pratiques de sécurité spécifiquement adaptées à la programmation en PHP. Il couvre les aspects traités dans cette alerte.

Gestion détaillée du document

09 septembre 2003 version initiale.