

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Exploitation massive d'une faille du forum phpBB

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-2004-ALE-014>

Gestion du document

Référence	CERTA-2004-ALE-014
Titre	Exploitation massive d'une faille du forum phpBB
Date de la première version	22 décembre 2004
Date de la dernière version	–
Source(s)	Alerte US CERT TA04-356A du 21 décembre 2004
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

Tout système avec un forum phpBB en version 2.0.10 ou antérieure.

3 Description

phpBB est un outil de mise en place de forum en source ouverte facilement configurable. Ce forum, basé sur le langage php, peut être installé sur différents types de serveur http (Apache, IIS, ...) et peut interagir avec plusieurs types de bases de données (MySQL, PostgreSQL, Microsoft SQL Server, Microsoft Access, ...).

Une vulnérabilité de type « injection SQL » (voir la note d'information CERTA-2004-INF-001) est présente dans le fichier `viewtopic.php`. En insérant la séquence de caractères `%2527` dans le paramètre `highlight` du fichier `viewtopic.php`, il est possible d'exécuter du code arbitraire à distance sur le serveur hébergeant le forum. Une exploitation visible de cette vulnérabilité peut être la défiguration d'un site web.

Un ver nommé `Santy.A` se propage en exploitant cette faille. Lorsqu'il infecte un système, il tente de remplacer les fichiers avec une extension en `.htm`, `.php`, `.asp`, `.shtm`, `.jsp` et `.phtm` afin de réaliser la défiguration du site. Il se copie dans un fichier nommé `m1h020f`. Le ver peut ensuite se propager si l'interpréteur `perl` est installé.

La tentative d'exploitation de cette vulnérabilité laisse des traces significatives dans les journaux, notamment le fragment `highlight=%2527`.

4 Solution

Mettre à jour phpBB en version 2.0.11 :

<http://www.phpbb.com/downloads.php>

5 Documentation

- Note d'information CERTA-2004-INF-001 : Sécurité des applications Web et vulnérabilité de type « injection de données »

<http://www.certa.ssi.gouv.fr/site/CERTA-2004-INF-001>

- Bulletin d'alerte de l'US CERT TA04-356A du 21 décembre 2004

<http://www.us-cert.gov/cas/techalerts/TA04-356A.html>

Gestion détaillée du document

22 décembre 2004 version initiale.