

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités de 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-2005-AVI-086>

Gestion du document

Référence	CERTA-2005-AVI-086
Titre	Vulnérabilités de phpBB
Date de la première version	24 février 2005
Date de la dernière version	–
Source(s)	Bulletins de sécurité iDefense du 22 février 2005
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

- Atteinte à la confidentialité des fichiers ;
- atteinte à l'intégrité des fichiers.

2 Systèmes affectés

phpBB versions 2.0.11 et antérieures.

3 Résumé

Deux vulnérabilités ont été découvertes dans l'outil *phpBB*.

4 Description

L'outil *phpBB* est utilisé pour la mise en place de forums sur l'Internet.

La première vulnérabilité (CVE CAN-2005-0258) concerne la fonction *usercp_register.php*. Un utilisateur distant mal intentionné peut exploiter cette vulnérabilité pour détruire des fichiers arbitraires sur le système.

La deuxième vulnérabilité (CVE CAN-2005-0259) concerne la gestion de variables relatives à l'image *avatar* (image associée à un nom d'utilisateur). Un utilisateur ayant un compte sur le serveur cible peut exploiter cette vulnérabilité pour accéder en lecture à n'importe quel fichier du système.

5 Contournement provisoire

La première vulnérabilité ne pourra pas être exploitée si la galerie des images *avatar* est désactivée.

La deuxième vulnérabilité ne pourra pas être exploitée si les images *avatar* distantes et le téléchargement de ces images *avatar* sont désactivés.

6 Solution

La version 2.0.12 de *phpBB* corrige ces vulnérabilités.

7 Documentation

- Site Internet de l'outil *phpBB* :
<http://www.phpbb.com>
- Bulletin de sécurité iDefense du 22 février 2005 (CVE CAN-2005-0258) :
<http://www.iddefense.com/application/poi/display?id=205&type=vulnerabilities>
- Bulletin de sécurité iDefense du 22 février 2005 (CVE CAN-2005-0259) :
<http://www.iddefense.com/application/poi/display?id=204&type=vulnerabilities>
- Bulletin de sécurité FreeBSD pour *phpBB* du 23 février 2005 :
<http://www.vuxml.org/freebsd/pkg-phpbb.html>
- Référence CVE CAN-2005-0258 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0258>
- Référence CVE CAN-2005-0259 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0259>

Gestion détaillée du document

24 février 2005 version initiale.