

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans 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-096>

Gestion du document

Référence	CERTA-2005-AVI-096-001
Titre	Vulnérabilités dans phpBB
Date de la première version	02 mars 2005
Date de la dernière version	11 juillet 2005
Source(s)	Message posté sur le site de phpBB le 27 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

- Obtention des droits de l'administrateur du forum ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

phpBB versions 2.0.12 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, présente dans le fichier `sessions.php`, permet d'obtenir les droits de l'administrateur du forum. La seconde vulnérabilité, présente dans le fichier `viewtopic.php`, permet de visualiser l'arborescence du répertoire web.

5 Solution

La version 2.0.13 corrige ces vulnérabilités.

6 Documentation

- Site de phpBB :
<http://www.phpbb.com>
- Message posté sur le site de phpBB le 27 février 2005 :
<http://www.phpbb.com/phpBB/viewtopic.php?f=14&t=267563>
- Bulletin de sécurité iDEFENSE id=204 du 02.22.05 :
<http://www.odefense.com/application/poi/display?id=204&type=vulnerabilities>
- Bulletin de sécurité iDEFENSE id=205 du 02.22.05 :
<http://www.odefense.com/application/poi/display?id=205&type=vulnerabilities>
- Bulletins de sécurité FreeBSD du 28 février 2005 et du 09 juillet 2005 :
<http://www.vuxml.org/freebsd/pkg-phpbb.html>
- Bulletin de sécurité Gentoo GLSA 2005:03-02 du 01 mars 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200503-02.xml>
- 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

02 mars 2005 version initiale.

11 juillet 2005 ajout des bulletins de sécurité iDEFENSE id=204 et id=205, du bulletin supplémentaire FreeBSD ainsi que des références CVE CAN-2005-0258 et CVE CAN-2005-0259.