

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité 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-426>

---

### Gestion du document

Référence	CERTA-2005-AVI-426-001
Titre	Vulnérabilités de phpBB
Date de la première version	31 octobre 2005
Date de la dernière version	22 décembre 2005
Source(s)	Message posté sur le site de phpBB le 30 octobre 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

Injection de code.

## 2 Systèmes affectés

phpBB versions 2.0.17 et antérieures.

## 3 Description

L'outil phpBB est utilisé dans la mise en œuvre de forums sur l'Internet.

Quelques vulnérabilités ont été découvertes dans le fichier `usercp_register.php`, permettant d'injecter du code.

## 4 Solution

La version 2.0.18 corrige ces vulnérabilités. phpBB peut se télécharger à l'adresse suivante :  
<http://www.phpbb.com/downloads.php>

## 5 Documentation

- Site Internet de phpBB :  
<http://www.phpbb.com>
- Message posté sur le site de phpBB le 30 octobre 2005 :  
<http://www.phpbb.com/phpBB/viewtopic.php?f=14&t=336756>
- Bulletin de sécurité Debian DSA-925 du 22 décembre 2005 :  
<http://www.debian.org/security/2005/dsa-925>
- Référence CVE CVE-2005-3310 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3310>
- Référence CVE CVE-2005-3415 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3415>
- Référence CVE CVE-2005-3416 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3416>
- Référence CVE CVE-2005-3417 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3417>
- Référence CVE CVE-2005-3418 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3418>
- Référence CVE CVE-2005-3419 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3419>
- Référence CVE CVE-2005-3420 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3420>
- Référence CVE CVE-2005-3536 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3536>
- Référence CVE CVE-2005-3537 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3537>

## Gestion détaillée du document

**31 octobre 2005** version initiale.

**22 décembre 2005** ajout du site de téléchargement de phpBB, de la référence au bulletin de sécurité Debian DSA-925 et des références CVE.