



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 12 juin 2006  
N° CERTA-2006-AVI-235

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans Wordpress

---

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-2006-AVI-235>

---

### Gestion du document

|                             |                               |
|-----------------------------|-------------------------------|
| Référence                   | CERTA-2006-AVI-235            |
| Titre                       | Vulnérabilités dans Wordpress |
| Date de la première version | 12 juin 2006                  |
| 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

Une vulnérabilité dans le logiciel de gestion de contenu Wordpress peut-être exploitée afin de compromettre un système vulnérable.

## 2 Systèmes affectés

Wordpress versions 2.x

## 3 Résumé

Lors de l'enregistrement d'un profil utilisateur ou à l'occasion de la mise à jour d'un profil, une erreur dans le script PHP peut être exploitée pour injecter et exécuter du code arbitraire.

## 4 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

## 5 Documentation

- Bulletin de sécurité de l'éditeur
- <http://wordpress.org/download/>
- Bulletin de sécurité Gentoo GLSA-200606-08.XML du 12 juin 2006 :  
<http://www.gentoo.org/security/en/glsa/glsa-200606-08.xml>
- Référence CVE CAN-2006-2702 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-2702>
- Référence CVE CAN-2006-2667 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-2667>

### Gestion détaillée du document

**12 juin 2006** version initiale.