

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité 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-2008-AVI-060>

---

### Gestion du document

|                             |   |
|-----------------------------|---|
| Référence                   | CERTA-2008-AVI-060  |
| Titre                       | Vulnérabilité dans WordPress                              |
| Date de la première version | 08 février 2008   |
| Date de la dernière version | –   |
| Source(s)                   | Bulletin de mise à jour WordPress 2.3.3 du 5 février 2008 |
| 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 l'intégrité des données.

## 2 Systèmes affectés

Les versions antérieures à la 2.3.3.

## 3 Résumé

Une vulnérabilité non publiée touche WordPress lorsque l'enregistrement en ligne est disponible.

## 4 Description

Le module `xmplrpc.php` permet à l'aide d'une requête spécifiquement créée de modifier les messages d'autres utilisateurs.

## **5 Solution**

Mettre à jour en version 2.3.3 (cf. section Documentation).

## **6 Documentation**

- Alerte de Secunia numéro 27669 du 07 février 2008 :  
<http://secunia.com/advisories/27669/>
- Notes de mise à jour WordPress 2.3.3 du 5 février 2008 :  
<http://wordpress.org/development/2008/02/wordpress-233/>
- Bulletin du NIST CVE-2008-0664 du 07 février 2008 :  
<http://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-0664>

## **Gestion détaillée du document**

**08 février 2008** version initiale.