Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 23 mai 2006
N° CERTA-2006-AVI-213

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Xoops

Gestion du document

Référence	CERTA-2006-AVI-213
Titre	Vulnérabilité dans Xoops
Date de la première version	23 mai 2006
Date de la dernière version	–
Source(s)	Correctif de sécurité du projet Xoops
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

- Contournement de la politique de sécurité ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

La version 2.0.13.2 de Xoops, ainsi que celles antérieures.

3 Résumé

Une vulnérabilité a été identifiée dans Xoops. Des utilisateurs malveillants distants peuvent l'utiliser pour accéder à des informations sur le système où Xoops fonctionne, ou injecter dans certaines conditions du code PHP.

4 Description

Xoops est un système dynamique de gestion de contenu écrit en PHP, et pouvant servir au développement de sites Internet. Une vulnérabilité concernant la version 2.0.13.2 et celles antérieures peut permettre à un utilisateur

malveillant de contourner la politique de sécurité. Plus précisément, Ces versions ne vérifient pas correctement les valeurs attribuées au paramètre `xoopsConfig`. Il est alors possible :

1. de récupérer des fichiers locaux à la machine où Xoops fonctionne en envoyant une requête particulière ;
2. d'injecter du code PHP dans certains fichiers journaux d'Apache ou dans des images *avatars* (images associées aux noms d'utilisateurs).

Ces deux actions sont possibles si le serveur Xoops est configuré avec l'option `register_globals`.

5 Solution

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

6 Documentation

- Site du projet Xoops :
  http://www.frxoops.org
- Bulletin de sécurité du projet Xoops du 23 mai 2006 :
  http://www.frxoops.org/modules/news/article.php?storyid=1007

Gestion détaillée du document

23 mai 2006 version initiale.