Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 juin 2008
N° CERTA-2008-AVI-311

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans TYPO3

Gestion du document

Référence	CERTA-2008-AVI-311
Titre	Vulnérabilités dans TYPO3
Date de la première version	13 juin 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité TYPO320080611-1 du 11 juin 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

- Exécution de code arbitraire à distance ;
- injection de code indirecte (*cross-site scripting*).

2 Systèmes affectés

- *TYPO3* versions 3.x ;
- *TYPO3* versions 4.0 à 4.0.8 ;
- *TYPO3* versions 4.1 à 4.1.6 ;
- *TYPO3* version 4.2.0.

3 Résumé

Deux vulnérabilités dans *TYPO3* permettent l'exécution de code arbitraire à distance et la réalisation d'attaques de type *cross-site scripting*.

4 Description

Deux vulnérabilités ont été découvertes dans *TYPO3* :

- la valeur par défaut de la variable `fileDenyPattern` (liée configuration *TYPO3*) permet à des utilisateurs authentifiés de télécharger sur le serveur *Apache* des fichiers de configuration (`.htaccess`). De plus, si le module `mod_mime` est activé sur le serveur *Apache*, les utilisateurs authentifiés peuvent installer ou créer des fichiers contenant du code `PHP` ;
- les données traitées par le fichier `fe_adminlib.inc` ne sont pas correctement filtrées. Cette vulnérabilité peut être exploitée pour réaliser des attaques de type *cross-site scripting*.

5 Solution

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

6 Documentation

- Bulletin de sécurité TYPO320080611-1 du 11 juin 2008 :
  http://typo3.org/teams/security/security-bulletins/typo3-20080611-1/

Gestion détaillée du document

13 juin 2008 version initiale.