Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 24 février 2010
N° CERTA-2010-AVI-091

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans TYPO3

Gestion du document

Référence	CERTA-2010-AVI-091
Titre	Vulnérabilités dans TYPO3
Date de la première version	24 février 2010
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

- Contournement de la politique de sécurité ;
- atteinte à la confidentialité des données ;
- injection de code indirecte à distance.

2 Systèmes affectés

TYPO3 versions 4.2.x et 4.3.x.

3 Résumé

Plusieurs vulnérabilités de TYPO3 permettent à un utilisateur malveillant de contourner la politique de sécurité, d'accéder à des données sensibles ou de réaliser de l'injection de code indirecte.

4 Description

Plusieurs vulnérabilités de TYPO3 ont été publiée :

- dans le module *backend*, un utilisateur authentifié peut, dans certaines conditions, accéder à des données d'autres utilisateurs de ce module ;

– ce même module permet à un utilisateur authentifié de réaliser de l'injection de code indirecte (XSS) ;
– quand TYPO3 est exécuter comme CGI sur PHP, une adresse réticulaire malveillante donnée en argument au script *index.php* permet de provoquer l'émission d'un message d'erreur avec injection de code HTML ;
– l'extension *saltedpasswords*, non active par défaut, permet, dans certaines circonstances, à un utilisateur malveillant de se connecter sans connaître le mot de passe.

5 Solution

Les versions 4.2.12 et 4.3.2 de TYPO3 remédient à ces vulnérabilités.
Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

– Bulletin de sécurité TYPO3 du 23 février 2010 :
http://typo3.org/teams/security/security-bulletins/typo3-sa-2010-004/

Gestion détaillée du document

24 février 2010 version initiale.