

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités de TYPO3

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-2009-AVI-063>

Gestion du document

Référence	CERTA-2009-AVI-063
Titre	Vulnérabilités de TYPO3
Date de la première version	11 février 2009
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

- Exécution de code arbitraire à distance ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

TYPO3 versions 3.x et 4.x

3 Résumé

Des vulnérabilités dans TYPO3 permettent à un utilisateur malveillant d'exécuter du code à distance et de porter atteinte à la confidentialité de données.

4 Description

Deux vulnérabilités de TYPO3 sont publiées :

- la première réside dans un défaut de validation de données entrées par l'utilisateur. Elle permet à un utilisateur malveillant de réaliser de l'injection de code indirecte (XSS ou *cross-site scripting*) ;

- la deuxième réside dans une faiblesse du mécanisme de suivi des accès aux pages, *jumpUrl*. Son exploitation permet à un utilisateur malveillant non authentifié de lire des informations sensibles. L'attaquant peut également exécuter du code arbitraire à distance.

Un code d'exploitation de la seconde vulnérabilité est disponible sur l'internet.

5 Solution

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

6 Documentation

- Bulletin de sécurité TYPO3-SA-2009-002 du 10 février 2009 :
<http://typo3.org/teams/security/security-bulletins/typo3-sa-2009-002/>

Gestion détaillée du document

11 février 2009 version initiale.