Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 26 octobre 2009
N° CERTA-2009-AVI-454

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans TYPO3

Gestion du document

Référence	CERTA-2009-AVI-454
Titre	Multiples vulnérabilités dans TYPO3
Date de la première version	26 octobre 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité TYPO3-SA-2009-016 du 22 octobre 2009
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 ;
- contournement de la politique de sécurité ;
- injection de code indirecte.

2 Systèmes affectés

- *TYPO3* versions 4.0.13 et antérieures ;
- *TYPO3* versions 4.1.12 et antérieures ;
- *TYPO3* versions 4.2.9 et antérieures ;
- *TYPO3* versions 4.3.0beta1 et antérieures.

3 Résumé

De multiples vulnérabilités dans *TYPO3* permettent d'exécuter du code arbitraire à distance, de réaliser diverses injections de code ou d'obtenir un accès à l'outil d'installation.

4 Description

De multiples vulnérabilités ont été découvertes dans *TYPO3* :

- plusieurs problèmes affectent le *backend*. Elles permettent de recalculer la clé de chiffrement, de réaliser diverses injections de code indirectes, ou d'exécuter des commandes arbitraires sur le système. Ces vulnérabilités nécessitent toutes de disposer d'un compte valide ;
- une injection `SQL` est possible via la fonctionnalité d'édition du *frontend*. Cette vulnérabilité requiert un compte valide ;
- du code `HTML` ou `JavaScript` peut être inséré via la fonction `t3lib_div::quoteJSvalue` ;
- une injection de code indirecte est possible via l'interface de connexion au *frontend* (`felogin`) ;
- il est possible de se connecter à l'outil d'installation en ne connaissant que l'empreinte `MD5` du mot de passe, ainsi que de réaliser des injections de code indirectes au travers de ce même outil.

5 Solution

Mettre à jour en version 4.1.13, 4.2.10 ou 4.3beta2, conformément au bulletin de sécurité de l'éditeur (cf. section Documentation). La branche 4.0 n'est plus maintenue. Le support pour la branche 4.1 ne sera plus assuré quand la version 4.3 sortira (prévue pour fin novembre 2009).

6 Documentation

- Bulletin de sécurité TYPO3-SA-2009-016 du 22 octobre 2009 :
  http://typo3.org/teams/security/security-bulletins/typo3-sa-2009-016/

Gestion détaillée du document

26 octobre 2009 version initiale.