



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 décembre 2010
N° CERTA-2010-AVI-614

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans 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-2010-AVI-614>

Gestion du document

Référence	CERTA-2010-AVI-614
Titre	Multiples vulnérabilités dans TYPO3
Date de la première version	17 décembre 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité TYPO3-SA-2010-022 du 16 décembre 2010
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 ;
- atteinte à la confidentialité des données ;
- injection de code indirecte à distance.

2 Systèmes affectés

- TYPO3 versions 4.2.15 et antérieures ;
- TYPO3 versions 4.3.8 et antérieures ;
- TYPO3 versions 4.4.4 et antérieures.

3 Résumé

De multiples vulnérabilités dans TYPO3 permettent, entre autres, d'exécuter du code arbitraire à distance.

4 Description

De multiples vulnérabilités ont été découvertes dans *TYPO3* :

- une injection de code indirecte est possible dans le *frontend* si la fonctionnalité *caching framework* est activée (les versions 4.2.x ne sont pas concernées) ;
- un utilisateur légitime du *backend* peut injecter du code HTML ou javascript ;
- il est possible de contourner la vérification des données transmises par les utilisateurs (mécanisme de protection contre les inclusions de fichiers PHP), ce qui permet l'exécution de code arbitraire à distance ;
- un utilisateur légitime pouvant utiliser les outils d'installation peut réaliser plusieurs injections de code indirectes ;
- des remontées de répertoires sont possibles via la bibliothèque `unzip` ;
- un utilisateur légitime du *backend* peut réaliser injection SQL via le module `list` ;
- dans une configuration SQL particulière (mode `NO_BACKSLASH_ESCAPES`), il est possible de faire des requêtes `LIKE` avec des jokers, ce qui permet d'avoir accès à des enregistrements théoriquement inaccessibles.

5 Solution

Les versions 4.2.16, 4.3.9 et 4.4.5 de *TYPO3* corrigent ces vulnérabilités.

6 Documentation

- Bulletin de sécurité TYPO3-SA-2010-022 du 16 décembre 2010 :
<http://typo3.org/teams/security/security-bulletins/typo3-sa-2010-022/>

Gestion détaillée du document

17 décembre 2010 version initiale.