

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-2011-AVI-432>

Gestion du document

Référence	CERTA-2011-AVI-432
Titre	Multiples vulnérabilités dans TYPO3
Date de la première version	09 août 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité TYPO3 TYPO3-CORE-SA-2011-001 du 27 juillet 2011
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 l'intégrité des données ;
- atteinte à la confidentialité des données ;
- injection de code indirecte à distance.

2 Systèmes affectés

- TYPO3 version 4.3.11 et antérieures ;
- TYPO3 version 4.4.8 et antérieures ;
- TYPO3 version 4.5.3 et antérieures.

3 Résumé

De multiples vulnérabilités dans TYPO3 permettent, entre autres, d'effectuer de l'injection de code indirecte à distance ou de porter atteinte à la confidentialité et à l'intégrité des données.

4 Description

De multiples vulnérabilités ont été découvertes dans TYPO3 :

- plusieurs injections de code indirecte à distance sont possibles ;
- un utilisateur s’authentifiant avec des identifiants erronés recevra des entêtes *HTTP* différents selon qu’il ait fourni un nom d’utilisateur correct ou non ;
- un utilisateur peut contourner le délai d’attente imposé après avoir fourni des identifiants incorrects ;
- la fonctionnalité `getText` peut être utilisée pour récupérer des données arbitraires depuis la base de données TYPO3 ;
- une vulnérabilité liée à l’utilisation de la fonction `Unserialize()` permet d’effacer arbitrairement les fichiers auxquels le serveur Web a accès.

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 TYPO3-CORE-SA-2011-001 du 27 juillet 2011 :
<http://typo3.org/teams/security/security-bulletins/typo3-core/typo3-core-sa-2011-001/>

Gestion détaillée du document

09 août 2011 version initiale.