



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 octobre 2010
N° CERTA-2010-AVI-474-001

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-474>

Gestion du document

Référence	CERTA-2010-AVI-474-001
Titre	Multiples vulnérabilités dans TYPO3
Date de la première version	07 octobre 2010
Date de la dernière version	27 octobre 2010
Source(s)	Bulletin de sécurité TYPO3-SA-2010-020 du 06 octobre 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

- Déni de service à distance ;
- atteinte à la confidentialité des données ;
- élévation de privilèges ;
- injection de code indirecte à distance.

2 Systèmes affectés

- TYPO3 versions 4.2.x antérieures à 4.2.15 ;
- TYPO3 versions 4.3.x antérieures à 4.3.7 ;
- TYPO3 versions 4.4.x antérieures à 4.4.4.

3 Résumé

De multiples vulnérabilités dans TYPO3 permettent un déni de service à distance, la lecture de certains fichiers du système, une élévation de privilèges et une injection de code indirecte à distance.

4 Description

De multiples vulnérabilités ont été découvertes dans *TYPO3* :

- une faille permet le contournement du mécanisme `jumpUrl`, dont la fonctionnalité est de vérifier les droits d'accès à des pages ou des fichiers. L'exploitation de cette vulnérabilité permet de lire tout fichier auquel le compte ayant lancé le serveur Web a accès ;
- une injection de code indirecte est possible via le *backend* de *TYPO3*. Il est néanmoins nécessaire de disposer d'un compte autorisé à se connecter au *backend* pour pouvoir exploiter cette vulnérabilité ;
- une faille dans le gestionnaire d'extensions permet de lire les fichiers auxquels le serveur Web a accès. Il est nécessaire de disposer d'un compte d'administrateur pour pouvoir exploiter cette vulnérabilité ;
- la tâche `be_user_creation` permet de créer des utilisateurs qui sont membres de groupes arbitraires et par ce biais, d'élever les privilèges. L'exploitation de cette vulnérabilité requiert des droits de création d'utilisateurs dans le centre de tâches ;
- un problème dans la fonction PHP `filter_var()` permet la réalisation d'un déni de service à distance lorsque la fonction `htmlspecialchars::validEmail()` est utilisée ;
- une injection de code indirecte est possible via la fonction `RemoveXSS`.

5 Solution

Mettre à jour *TYPO3* en version 4.2.15, 4.3.7 ou 4.4.4.

6 Documentation

- Bulletin de sécurité TYPO3-SA-2010-020 du 06 octobre 2010 :
<http://typo3.org/teams/security/security-bulletins/typo3-sa-2010-020/>
- Référence CVE CVE-2010-3710 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3710>
- Référence CVE CVE-2010-3714 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3714>
- Référence CVE CVE-2010-3715 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3715>
- Référence CVE CVE-2010-3716 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3716>
- Référence CVE CVE-2010-3717 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3717>
- Référence CVE CVE-2010-4068 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4068>

Gestion détaillée du document

07 octobre 2010 version initiale.

27 octobre 2010 ajout des références CVE.