Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 30 mars 2012
N° CERTA-2012-AVI-181

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans TYPO3

Gestion du document

Référence	CERTA-2012-AVI-181
Titre	Multiples vulnérabilités dans TYPO3
Date de la première version	30 mars 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité TYPO3 sa-2012-001 du 28 mars 2012
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

- Atteinte à la confidentialité des données ;
- injection de code indirecte à distance.

2 Systèmes affectés

Versions antérieures à TYPO3 4.4.14, 4.5.14 et 4.6.7.

3 Résumé

Quatre vulnérabilités ont été corrigées dans TYPO3.

4 Description

Une exploitation de ces vulnérabilités peut conduire à des fuites d'informations et à des injections de codes à distance (*XSS*). Parmi ces failles une affecte la fonction *t3lib_div::RemoveXSS()* lors du filtrage de certains caractères *HTML* spécifiques. La deuxième est, elle aussi, de type *XSS* mais requiert d'avoir un accès utilisateur sur l'application. La troisième donne directement accès au CLI (*Command Line Interface*) et permet de découvrir

le nom de la base de données TYPO3. Enfin la dernière permet de "dé-sérialiser" arbitrairement des objets de TYPO3.

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-2012-001 du 28 mars 2012 :
  http://typo3.org/teams/security/security-bulletins/typo3-core/typo3-core-sa-2012-001/
- Référence CVE CVE-2012-1605 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1605
- Référence CVE CVE-2012-1606 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1606
- Référence CVE CVE-2012-1607 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1607
- Référence CVE CVE-2012-1608 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1608

Gestion détaillée du document

30 mars 2012 version initiale.