



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 janvier 2009
N° CERTA-2009-AVI-024

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-2009-AVI-024>

Gestion du document

Référence	CERTA-2009-AVI-024
Titre	Multiples vulnérabilités dans TYPO3
Date de la première version	21 janvier 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité TYPO3-SA-2009-001
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 commandes arbitraires à distance ;
- injections de code indirectes ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- TYPO3 versions 4.0.0 à 4.0.9 ;
- TYPO3 versions 4.1.0 à 4.1.7 ;
- TYPO3 versions 4.2.0 à 4.2.3.

3 Résumé

De multiples vulnérabilités dans TYPO3 permettent une exécution de commandes arbitraires à distance, diverses injections de code indirectes ou un contournement de la politique de sécurité.

4 Description

De multiples vulnérabilités ont été découvertes dans *TYPO3* :

- la clé de chiffrement utilisée par *TYPO3* a une faible entropie ;
- les jetons de session ne sont pas correctement invalidés et peuvent être rejoués ;
- le moteur de recherche indexée ne filtre pas correctement les paramètres, ce qui permet une exécution de commandes arbitraires à distance. Par ailleurs, le nom et le contenu des fichiers à indexer ne sont pas non plus correctement filtrés, ce qui permet de réaliser des attaques de type *cross-site scripting* ;
- des attaques de type *cross-site scripting* sont possibles via les composants ADOdb et Workspace.

5 Solution

Mettre à jour *TYPO3* en version 4.0.10, 4.1.8 ou 4.2.4. L'application des mises à jour ne suffit pas à corriger toutes les vulnérabilités, il est également nécessaire de créer une nouvelle clé de chiffrement. Cette procédure est décrite dans le bulletin de sécurité de l'éditeur (voir section Documentation).

6 Documentation

- Bulletin de sécurité TYPO3-SA-2009-001 :
<http://typo3.org/teams/security/security-bulletins/typo3-sa-2009-001/>
- Référence CVE CVE-2009-0255 :
<http://cve.mitre.org/cgi-bin/cvename.cge?name=CVE-2009-255>
- Référence CVE CVE-2009-0256 :
<http://cve.mitre.org/cgi-bin/cvename.cge?name=CVE-2009-256>
- Référence CVE CVE-2009-0257 :
<http://cve.mitre.org/cgi-bin/cvename.cge?name=CVE-2009-257>
- Référence CVE CVE-2009-0258 :
<http://cve.mitre.org/cgi-bin/cvename.cge?name=CVE-2009-258>

Gestion détaillée du document

21 janvier 2009 version initiale.