Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 janvier 2008
N° CERTA-2008-AVI-021

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Drupal

Gestion du document

Référence	CERTA-2008-AVI-021
Titre	Vulnérabilités dans Drupal
Date de la première version	15 janvier 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Drupal SA-2008-005 du 10 janvier 2008 Bulletin de sécurité Drupal SA-2008-006 du 10 janvier 2008 Bulletin de sécurité Drupal SA-2008-007 du 10 janvier 2008
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

Injections de code indirectes (*cross-site scripting* et *cross-site request forgery*).

2 Systèmes affectés

- *Drupal* versions 4.x antérieures à 4.7.11 ;
- *Drupal* versions 5.x antérieures à 5.6.

3 Résumé

Plusieurs vulnérabilités dans *Drupal* permettent de réaliser diverses injections de code indirectes.

4 Description

Plusieurs vulnérabilités ont été découvertes dans *Drupal* :

- une vulnérabilité dans le module de traitement des flux `RSS` permet de réaliser une attaque de type *cross-site request forgery* (SA-2008-005) ;
- l'utilisation de séquences de caractères considérés comme invalides par les spécifications de `UTF8` permet de réaliser une attaque de type *cross-site scripting* (SA-2008-006) ;
- lorsque les fichiers de thème (`.tpl.php`) ont des droits d'accès via le Web et que la variable `PHP register_globals` est activée, il est possible de réaliser des attaques de type *cross-site scripting* (SA-2008-007).

5 Contournement provisoire

Il n'existe pas de correctif pour la vulnérabilité décrite dans l'avis *Drupal* SA-2008-007. L'éditeur recommande de désactiver la variable `register_globals` et de ne pas positionner de droits d'accès via le Web sur les fichiers de thème.

6 Solution

Mettre à jour en version 4.7.11 ou 5.6. Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

7 Documentation

- Bulletin de sécurité Drupal SA-2008-005 du 10 janvier 2008 :
  http://drupal.org/node/208562
- Bulletin de sécurité Drupal SA-2008-006 du 10 janvier 2008 :
  http://drupal.org/node/208564
- Bulletin de sécurité Drupal SA-2008-007 du 10 janvier 2008 :
  http://drupal.org/node/208565

Gestion détaillée du document

15 janvier 2008 version initiale.