

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Drupal

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-108>

Gestion du document

Référence	CERTA-2010-AVI-108
Titre	Multiples vulnérabilités dans Drupal
Date de la première version	05 mars 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Drupal SA-CORE-2010-001 du 03 mars 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

- Contournement de la politique de sécurité ;
- injection de code indirecte à distance.

2 Systèmes affectés

- *Drupal* versions 6.x antérieures à 6.16 ;
- *Drupal* versions 5.x antérieures à 5.22.

3 Résumé

De multiples vulnérabilités dans *Drupal* permettent de réaliser des injections de code indirectes et de contourner la politique de sécurité.

4 Description

De multiples vulnérabilités ont été découvertes dans *Drupal* :

- une injection de code indirecte est possible durant l'installation (cette vulnérabilité n'affecte que *Drupal* 6) ;

- la fonction `drupal_goto()` est censée rediriger les utilisateurs vers une autre page du même site *Drupal*. Néanmoins, une faiblesse dans cette fonction permet de rediriger les utilisateurs vers un autre site externe, ce qui rend possible des attaques de type hameçonnage (*phishing*);
- des attaques de type injection de code indirecte sont possibles via le nom de langue transmis aux modules. Toutefois, l'exploitation de ces vulnérabilités nécessite de disposer de droits suffisants sur la gestion des langues;
- dans certains cas, un utilisateur ayant une session ouverte bloquée peut maintenir cette session.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Drupal SA-CORE-2010-001 du 03 mars 2010 :
<http://drupal.org/node/731710>

Gestion détaillée du document

05 mars 2010 version initiale.