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 mai 2011
N° CERTA-2011-AVI-321

**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-2011-AVI-321

## Gestion du document

| | |
|---|---|
| Référence | CERTA-2011-AVI-321 |
| Titre | Multiples vulnérabilités dans Drupal |
| Date de la première version | 30 mai 2011 |
| Date de la dernière version | – |
| Source(s) | Bulletin de sécurité Drupal SA-CORE-2011-001 du 25 mai 2011 |
| 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 7.x antérieures à 7.1 ;
- *Drupal* versions 6.x antérieures à 6.21.

## 3 Résumé

De multiples vulnérabilités dans *Drupal* permettent de réaliser des injections de code indirectes ou d'obtenir des accès à des fichiers privés.

## 4 Description

De multiples vulnérabilités ont été découvertes dans *Drupal* :

- une injection de code indirecte est possible du fait d'une faille dans le gestionnaire d'erreurs (*Drupal* 6.x) ;

– un problème dans le module des couleurs permet une injection de code indirecte (*Drupal* 6.x et 7.x) ;
– lorsque les fichiers privés sont utilisés avec un module d'accès aux noeuds, ils peuvent être accédés sans restriction via le module `File` (*Drupal* 7.x).

# 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-2011-001 du 25 mai 2011 :
http://drupal.org/node/1168756

# Gestion détaillée du document

**30 mai 2011** version initiale.