



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 14 août 2008  
N° CERTA-2008-AVI-418

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-2008-AVI-418>

---

### Gestion du document

Référence	CERTA-2008-AVI-418
Titre	Multiples vulnérabilités dans Drupal
Date de la première version	14 août 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Drupal SA-2008-047 du 13 août 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

- Exécution de code arbitraire à distance ;
- injection de code indirecte ;
- atteinte à l'intégrité des données.

## 2 Systèmes affectés

- *Drupal* versions 5.x antérieures à 5.10 ;
- *Drupal* versions 6.x antérieures à 6.4.

## 3 Résumé

De multiples vulnérabilités dans *Drupal* permettent de modifier le contenu, de réaliser des injections de code indirectes et de déposer des fichiers.

## 4 Description

De multiples vulnérabilités ont été découvertes dans *Drupal* :

- plusieurs erreurs permettent de réaliser des attaques de type *cross-site scripting* et *cross-site request forgery* ;
- le module `blogAPI` ne valide pas correctement l'extension des fichiers déposés ce qui permet à des utilisateurs disposant de droits spécifiques de déposer des fichiers dangereux ;
- le module `Upload` dans *Drupal 6* contient une vulnérabilité permettant l'élévation de privilèges pour certains utilisateurs disposant de droits spécifiques. Ceci permet notamment de modifier du contenu.

## 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-2008-047 du 13 août 2008 :  
<http://drupal.org/node/295053>

## Gestion détaillée du document

14 août 2008 version initiale.