



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 25 octobre 2006
N° CERTA-2006-AVI-464

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-2006-AVI-464>

Gestion du document

Référence	CERTA-2006-AVI-464
Titre	Multiples vulnérabilités dans Drupal
Date de la première version	25 octobre 2006
Date de la dernière version	–
Source(s)	Bulletins de sécurité Drupal du 18 octobre 2006
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

- Atteinte à l'intégrité des données ;
- Cross-site Scripting.

2 Systèmes affectés

- Drupal 4.7.3 ;
- Drupal 4.6.9.

3 Résumé

De multiples vulnérabilités sont présentes dans Drupal et permettent à un utilisateur distant d'altérer le contenu d'une page php ou de réaliser une attaque de type `cross-site scripting`.

4 Description

Trois vulnérabilités sont présentes dans Drupal :

- La première permet à un utilisateur distant de modifier la page de destination spécifiée dans un formulaire HTML afin, par exemple, de diriger la victime vers un site arbitraire ;

- la deuxième permet à un utilisateur distant, par le biais d'une page web construite de façon particulière, d'injecter une réponse dans un formulaire Drupal dans le contexte du navigateur d'un utilisateur consultant le site de l'attaquant ;
- la dernière vulnérabilité permet à un utilisateur distant de réaliser une attaque de type `cross-site scripting` via une vulnérabilité présente dans l'analyseur XML de Drupal.

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 du 18 octobre 2006 :
<http://drupal.org/security/>
- Bulletins de sécurité du port FreeBSD de Drupal du 18 octobre 2006 :
<http://www.vuxml.org/freebsd/pkg-drupal.html>

Gestion détaillée du document

25 octobre 2006 version initiale.