Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 26 mai 2006
N° CERTA-2006-AVI-219

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : 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-219

Gestion du document

Référence	CERTA-2006-AVI-219
Titre	Vulnérabilités dans Drupal
Date de la première version	26 mai 2006
Date de la dernière version	–
Source(s)	Bulletin de mise à jour du projet Drupal du 18 mai 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

- Exécution de code arbitraire à distance ;
- contournement de la politique de sécurité ;
- atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- La version 4.6.6 de Drupal et les versions antérieures ;
- la version 4.7.0 de Drupal.

3 Description

Drupal est un environnement pour gérer les contenus de sites Internet. Deux vulnérabilités ont été identifiées dans les versions 4.6.X et 4.7.0 :

- La première concerne les droits manquants au répertoire `files`. Un utilisateur malveillant peut donc lire ou écrire certains fichiers (voire même les exécuter s'il peut les télécharger au préalable sur le site vulnérable).
- La seconde repose sur un mauvais contrôle de paramètres intégrés dans des requêtes SQL. Il est alors possible pour un utilisateur malveillant d'injecter du code SQL arbitraire dans la base de données.

4 Solution

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

5 Documentation

- Bulletin de sécurité DRUPAL-SA-2006-005 du 18 mai 2006 :
  http://drupal.org/node/65357
- Bulletin de sécurité DRUPAL-SA-2006-006 du 24 mai 2006 :
  http://drupal.org/node/65409
- Mise à jour du projet Drupal :
  http://drupal.org/project

Gestion détaillée du document

26 mai 2006 version initiale.