



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 août 2010
N° CERTA-2010-AVI-386

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-386>

Gestion du document

Référence	CERTA-2010-AVI-386
Titre	Multiples vulnérabilités dans Drupal
Date de la première version	17 août 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité SA-CORE-2010-002 du 11 août 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

- Atteinte à la confidentialité des données ;
- contournement de la politique de sécurité ;
- injection de code indirecte à distance.

2 Systèmes affectés

- *Drupal* versions 6.x antérieures à 6.18 ;
- *Drupal* versions 5.x antérieures à 5.23.

3 Résumé

De multiples vulnérabilités dans *Drupal* permettent notamment de lire certains fichiers, de se connecter indûment et de réaliser des injections de code indirectes.

4 Description

De multiples vulnérabilités ont été découvertes dans *Drupal* :

- l'authentification par le module OpenID peut être contournée du fait d'un manque de vérifications. Cette vulnérabilité est présente dans les versions 6.x de *Drupal*. Les versions 5.x ne sont affectées que si le module tiers OpenID a été installé ;
- un utilisateur malintentionné peut déposer un fichier dont le nom correspond à un fichier existant déjà dans la base de données, à la casse près. Dans ce cas, un accès à l'autre fichier portant le même nom est accordé ;
- une vulnérabilité dans le module des commentaires permet de republier des commentaires n'apparaissant pas ;
- plusieurs injections de code indirectes existent dans divers modules (versions 6.x).

5 Solution

Les versions 5.23 et 6.18 ou 6.19 corrigent ces vulnérabilités. La version 6.19 ne corrige aucune vulnérabilité par rapport à la version 6.18.

6 Documentation

- Bulletin de sécurité SA-CORE-2010-002 du 11 août 2010 :
<http://drupal.org/node/880476>

Gestion détaillée du document

17 août 2010 version initiale.