



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 23 septembre 2009  
N° CERTA-2009-AVI-393

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-2009-AVI-393>

---

### Gestion du document

Référence	CERTA-2009-AVI-393
Titre	Multiples vulnérabilités dans Drupal
Date de la première version	23 septembre 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Drupal SA-CORE-2009-008 du 16 septembre 2009
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 ;
- accès non autorisé à un compte ;
- contournement de la politique de sécurité ;
- injection de requêtes illégitimes par rebond.

## 2 Systèmes affectés

- *Drupal* versions 5.x antérieures à 5.20 ;
- *Drupal* versions 6.x antérieures à 6.14.

## 3 Résumé

De multiples vulnérabilités dans *Drupal* permettent d'accéder de façon illégitime à des comptes et, dans certains cas, d'exécuter du code arbitraire à distance.

## 4 Description

De multiples vulnérabilités ont été découvertes dans *Drupal* :

- une injection de requêtes illégitimes par rebond permet d'ajouter des identités OpenID à des comptes actifs (versions 6.x) ;
- une erreur dans l'implémentation du module OpenID permet à un utilisateur d'accéder à un autre compte que le sien lorsqu'ils ont le même fournisseur OpenID 2.0 (versions 6.x) ;
- le dépôt de fichiers avec certaines extensions n'est pas correctement traité, ce qui permet une exécution de code arbitraire à distance. Toutefois, les fichiers sont stockés dans un répertoire protégé par un fichier `.htaccess` qui empêche leur exécution (sauf si le serveur *Apache* est configuré pour ignorer ces directives) (versions 6.x) ;
- l'identifiant de session n'est pas réinitialisé lorsqu'un utilisateur anonyme suit un lien lors d'une procédure de mot de passe oublié. Cet identifiant de session peut, sous certaines conditions, être rejoué (versions 5.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-2009-008 du 16 septembre 2009 :  
<http://drupal.org/node/579482>

## Gestion détaillée du document

23 septembre 2009 version initiale.