



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 11 juillet 2008
N° CERTA-2008-AVI-365

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-365>

Gestion du document

| | |
|-----------------------------|--|
| Référence | CERTA-2008-AVI-365 |
| Titre | Multiples vulnérabilités dans Drupal |
| Date de la première version | 11 juillet 2008 |
| Date de la dernière version | - |
| Source(s) | Bulletin de sécurité DRUPAL-SA-2008-044 du 09 juillet 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

- Contournement de la politique de sécurité ;
- injection de code indirecte ;
- injection SQL.

2 Systèmes affectés

- *Drupal* versions 5.x antérieures à 5.8 ;
- *Drupal* versions 6.x antérieures à 6.3.

3 Résumé

De multiples vulnérabilités dans *Drupal* permettent de réaliser diverses injections de code et d'obtenir un accès non autorisé.

4 Description

De multiples vulnérabilités ont été découvertes dans *Drupal* :

- plusieurs attaques de type *cross-site scripting* sont possibles dans *Drupal* versions 6.x ;
- des attaques de type *cross-site request forgery* ce qui peut entraîner l’effacement de certains éléments dans *Drupal* versions 5.x et 6.x ;
- en incitant sa victime à suivre un lien spécifiquement constitué, une personne malintentionnée peut obtenir un accès non autorisé à *Drupal* versions 5.x et 6.x ;
- des injections SQL sont possibles dans *Drupal* versions 6.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-2008-044 du 09 juillet 2008 :
<http://drupal.org/node/280571>

Gestion détaillée du document

11 juillet 2008 version initiale.