

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-2007-AVI-011>

Gestion du document

Référence	CERTA-2007-AVI-011
Titre	Multiples vulnérabilités dans Drupal
Date de la première version	08 janvier 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Drupal sa-2007-001 du 05 janvier 2007 Bulletin de sécurité Drupal sa-2007-002 du 05 janvier 2007
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

- Déni de service à distance ;
- attaques de type Cross Site Scripting.

2 Systèmes affectés

- Drupal 4.6.x ;
- Drupal 4.7.x.

3 Description

Plusieurs vulnérabilités découvertes dans Drupal permettent à un utilisateur malintentionné de provoquer un déni de service à distance ou de réaliser des attaques de types Cross Site Scripting.

Un utilisateur malveillant peut exploiter ces vulnérabilités afin d'inclure du code arbitraire sur le serveur. Ce code sera exécuté dans le contexte du navigateur Internet de l'utilisateur accédant au serveur vulnérable.

4 Solution

Appliquer les mises à jour de sécurité Drupal en passant à la version 4.6.11 ou 4.7.5 disponibles à l'adresse suivante :

<http://drupal.org/project/Drupal+project>

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

5 Documentation

- Site Internet Drupal :
<http://drupal.org/>
- Bulletin de sécurité Drupal sa-2007-001 du 05 janvier 2007 :
<http://drupal.org/files/sa-2007-001/advisory.txt>
- Bulletin de sécurité Drupal sa-2007-002 du 05 janvier 2007 :
<http://drupal.org/files/sa-2007-002/advisory.txt>
- Référence CVE CVE-2006-6646 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6646>
- Référence CVE CVE-2006-6647 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6647>

Gestion détaillée du document

08 janvier 2007 version initiale.