

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités du module Project de 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-054>

Gestion du document

Référence	CERTA-2007-AVI-054
Titre	Vulnérabilités du module Project de Drupal
Date de la première version	25 janvier 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité DRUPAL-SA-2007-004 du 23 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

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

2 Systèmes affectés

- Module Drupal Project *issue tracking* 4.7.x-2.1 ainsi que les versions antérieures ;
- Module Drupal Project *issue tracking* 4.7.x-1.1 ainsi que les versions antérieures ;
- Module Drupal Project 4.7.x-2.1 ainsi que les versions antérieures ;
- Module Drupal Project 4.7.x-1.1 ainsi que les versions antérieures ;
- Module Drupal Project *issue tracking* 5.x-0.x-dev antérieur à la version 5.x-0.1-beta ;
- Module Drupal Project 5.x-0.x-dev antérieur à la version 5.x-0.1-beta.

3 Description

Drupal est un système de gestion de contenu CMS (pour *Content Management System* fonctionnant avec des modules. Plusieurs vulnérabilités ont été identifiées dans l'un d'eux : le module `Project`. Celui-ci est utilisé dans la gestion des projets de sites Drupal. Il permet de les classer, de les renommer, et de contrôler le téléchargement des différentes versions.

Les permissions ne sont pas correctement manipulées par la fonction `project_issue_access()`. Il serait possible à une personne malveillante distante de récupérer tout fichier à télécharger, y compris ceux à accès restreint.

Une personne malveillante pourrait également exploiter certains champs, qui ne seraient pas correctement filtrés, entre autres par la fonction `check_plain()`, afin de lancer une attaque d'injection de code indirecte, ou *cross-site scripting*.

L'ajout de fichiers liés aux projets ne seraient pas correctement maîtrisés, et la politique de sécurité décrite dans le fichier `.htaccess FileInfo` pourrait donc être contournée pour ajouter de nouveaux fichiers avec n'importe quelle extension, comme `.php`, afin d'exécuter du code sur le serveur.

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 DRUPAL-SA-2007-004 du 23 janvier 2007 :
<http://drupal.org/node/112146>
- Présentation du module Project de Drupal :
<http://drupal.org/project/project>

Gestion détaillée du document

25 janvier 2007 version initiale.