

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-2012-AVI-052>

Gestion du document

Référence	CERTA-2012-AVI-052
Titre	Multiples vulnérabilités dans Drupal
Date de la première version	03 février 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité Drupal SA-CORE-2012-001 du 01 février 2012
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 ;
- injection de requêtes illégitime par rebond.

2 Systèmes affectés

- *Drupal* versions 6.x antérieures à 6.23 ;
- *Drupal* versions 7.x antérieures à 7.11.

3 Résumé

De multiples vulnérabilités dans *Drupal* permettent de contourner des restrictions d'accès à des fichiers, de modifier des informations d'utilisateur et d'injecter illégitimement des requêtes par rebond.

4 Description

De multiples vulnérabilités ont été découvertes dans *Drupal* :

- *OpenId* ne vérifie pas si certains attributs sont signés, ce qui permet de modifier les informations des utilisateurs (CVE-2012-0825) ;
- des injections de requêtes illégitimes par rebond sont possibles via le module *Aggregator*. Dans certains cas, l'exploitation de cette vulnérabilité permet de réaliser un déni de service (CVE-2012-0826) ;
- sous certaines conditions, des utilisateurs peuvent télécharger indûment des fichiers via le module *File*. Ce problème n'affecte que les versions 7.x de *Drupal* (CVE-2012-0827).

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-2012-001 du 01 février 2012 :
<http://drupal.org/node/1425084>
- Référence CVE CVE-2012-0825 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0825>
- Référence CVE CVE-2012-0826 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0826>
- Référence CVE CVE-2012-0827 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0827>

Gestion détaillée du document

03 février 2012 version initiale.