Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 février 2011
N° CERTA-2011-AVI-086-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Django

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-2011-AVI-086

Gestion du document

Référence	CERTA-2011-AVI-086-001
Titre	Multiples vulnérabilités dans Django
Date de la première version	14 février 2011
Date de la dernière version	16 février 2011
Source(s)	Bulletin de sécurité Django du 8 février 2011
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

- Atteinte à la confidentialité des données ;
- injection de code indirecte à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- Django 1.2.x versions inférieures à 1.2.5 ;
- Django 1.1.x versions inférieures à 1.1.4.

3 Résumé

Plusieurs vulnérabilités ont été corrigées dans Django. Celles-ci permettent de contourner la politique de sécurité, de réaliser une injection de code indirecte à distance et porter atteinte à la confidentialité des données.

4 Description

La première vulnérabilité corrigée permet de contourner la protection anti-injection de requêtes illégitimes par rebond. Une faille dans la gestion des noms de fichiers téléchargés vers le serveur permet à une personne malveillante de réaliser une injection de code indirecte à distance. Enfin, sur les systèmes Windows un attaquant capable de rejouer des connexions au serveur ou de contourner les mécanismes d'authentification peut afficher des fichiers arbitraires, à cause d'un problème dans l'utilisation des caractères de séparation du système de fichiers.

5 Solution

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

6 Documentation

- Bulletin de sécurité Django du 8 février 2011 :
  http://www.djangoproject.com/weblog/2011/feb/08/security/
- Bulletin de sécurité Debian DSA-2163-1 du 14 février 2011 :
  http://www.debian.org/security/2011/dsa-2163
- Référence CVE CVE-2011-0696 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0696
- Référence CVE CVE-2011-0697 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0697
- Référence CVE CVE-2011-0698 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0698

Gestion détaillée du document

14 février 2011 version initiale.

16 février 2011 ajout de la référence au bulletin Debian et des références CVE.