



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 septembre 2011
N° CERTA-2011-AVI-519

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-519>

Gestion du document

Référence	CERTA-2011-AVI-519
Titre	Multiples vulnérabilités dans Django
Date de la première version	15 septembre 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Django du 09 septembre 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

- Déni de service à distance ;
- atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données ;
- injection de requêtes illégitime par rebond.

2 Systèmes affectés

- Django 1.3.x ;
- Django 1.2.x.

3 Résumé

Plusieurs vulnérabilités dans Django permettent à une personne malintentionnée de porter atteinte à la confidentialité et l'intégrité des données, de provoquer un déni de service à distance ou d'injecter illégitimement des requêtes par rebond.

4 Description

Quatre vulnérabilités ont été découvertes dans Django :

- une erreur dans la gestion des données de session permet à une personne malintentionnée de porter à atteinte à l'intégrité de données de session ;
- une vulnérabilité dans le champ *URLField* permet une consommation excessive des ressources du système ;
- une erreur dans la validation des adresses réticulaires permet de porter atteinte à la confidentialité de certaines données ;
- une vulnérabilité dans le traitement des requêtes permet à une personne malintentionnée de corrompre la mémoire tampon.

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 09 septembre 2011 :
<https://www.djangoproject.com/weblog/2011/sep/09/security-releases-issued/>

Gestion détaillée du document

15 septembre 2011 version initiale.