Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 01 août 2012
N° CERTA-2012-AVI-412

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Django

Gestion du document

Référence	CERTA-2012-AVI-412
Titre	Vulnérabilités dans Django
Date de la première version	01 août 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité Django du 30 juillet 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

- Déni de service à distance ;
- injection de code indirecte à distance.

2 Systèmes affectés

- Django 1.3.x versions antérieures à 1.3.2 ;
- Django 1.4.x versions antérieures à 1.4.1.

3 Résumé

Trois vulnérabilités ont été corrigées dans Django. La première peut être exploitée par une personne malveillante pour effectuer de l'injection de code indirecte à distance (*XSS*). Les deux autres permettent de provoquer un déni de service à distance.

4 Solution

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

5 Documentation

- Bulletin de sécurité Django du 30 juillet 2012 :
  https://www.djangoproject.com/weblog/2012/jul/30/security-releases-issued/
- Référence CVE CVE-2012-3442 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3442
- Référence CVE CVE-2012-3443 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3443
- Référence CVE CVE-2012-3444 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3444

Gestion détaillée du document

01 août 2012 version initiale.