



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 juin 2011
N° CERTA-2011-AVI-339

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Ruby on Rails

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-339>

Gestion du document

Référence	CERTA-2011-AVI-339
Titre	Vulnérabilité dans Ruby on Rails
Date de la première version	14 juin 2011
Date de la dernière version	–
Source(s)	Notes des versions 2.3.12, 3.0.8 et 3.1.0.rc2 de Ruby on Rails du 08 juin 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

Injection de code indirecte à distance.

2 Systèmes affectés

- Ruby on Rails 3.0.x ;
- Ruby on Rails 2.3.x

3 Résumé

Une vulnérabilité de type injection de code indirecte à distance (XSS) a été identifiée dans Ruby on Rails.

4 Description

Ruby on Rails utilise un mécanisme de prévention des XSS en protégeant les chaînes de caractères présentées au client avant de les marquer comme étant *html safe*. Une vulnérabilité dans ce mécanisme permet de créer une chaîne *html safe* alors que celle-ci n'a pas été protégée, ce qui permet de provoquer une injection de code indirecte à distance.

5 Solution

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

6 Documentation

- Notes des versions 2.3.12, 3.0.8 et 3.1.0.rc2 de Ruby on Rails du 08 juin 2011 :
<http://weblog.rubyonrails.org/2011/6/8/potential-xss-vulnerability-in-ruby-on-rails-applications>

Gestion détaillée du document

14 juin 2011 version initiale.