



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 21 novembre 2011  
N° CERTA-2011-AVI-653

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-653>

---

### Gestion du document

Référence	CERTA-2011-AVI-653
Titre	Vulnérabilité dans Ruby on Rails
Date de la première version	21 novembre 2011
Date de la dernière version	–
Source(s)	Notes de mise à jour Rails du 18 novembre
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 versions 3.0.0 et supérieures ;
- Ruby on Rails versions 2.3.x utilisant le module d'extension rails\_xss.

## 3 Résumé

Une vulnérabilité permettant à une personne malintentionnée d'injecter indirectement du code à distance a été découverte dans *Ruby on Rails*.

## 4 Description

Une vulnérabilité a été découverte dans la méthode `translate` de *Ruby on Rails*. Elle permet à une personne malintentionnée d'effectuer 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 de mise à jour Rails du 18 novembre 2011 :  
<http://weblog.rubyonrails.org/2011/11/18/rails-3-1-2-has-been-released>  
<http://weblog.rubyonrails.org/2011/11/18/rails-3-0-11-has-been-released>
- Référence CVE CVE-2011-4319 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-4319>

## **Gestion détaillée du document**

**21 novembre 2011** version initiale.