

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités 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-083>

---

### Gestion du document

Référence	CERTA-2011-AVI-083
Titre	Multiples vulnérabilités dans Ruby on Rails
Date de la première version	10 février 2011
Date de la dernière version	–
Source(s)	Note de sortie des versions 2.3.11 et 3.0.4 de Ruby on Rails du 08 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

- Contournement de la politique de sécurité ;
- atteinte à l'intégrité des données ;
- injection de code indirecte à distance.

## 2 Systèmes affectés

- Ruby on Rails versions 2.3.10 et antérieures (CVE-2011-0446 à CVE-2011-0449) ;
- Ruby on Rails versions 3.0.3 et antérieures (CVE-2011-0448 et CVE-2011-0449 uniquement).

## 3 Résumé

Plusieurs vulnérabilités présentes dans Ruby on Rails permettent à un utilisateur distant de contourner la politique de sécurité, de porter atteinte à l'intégrité de données et de conduire des attaques de type injection de code indirecte à distance.

## 4 Description

Quatre vulnérabilités ont été identifiées dans Ruby on Rails.

La première et la deuxième, présentes dans les versions de la branche 2 et de la branche 3 de Ruby on Rails, permettent à un utilisateur de conduire des attaques de type injection de code indirecte à distance (CVE-2011-446 et CVE-2011-447).

La troisième et la quatrième, ne touchant que les versions de la branche 3, permettent à un utilisateur distant malintentionné de contourner certains filtrages du système (CVE-2011-448) et de réaliser des attaques de type injection SQL (CVE-2011-449).

## 5 Solution

Se référer à la note de sortie de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

## 6 Documentation

- Note de sortie des versions 2.3.11 et 3.0.4 de Ruby on Rails du 08 février 2011 :  
<http://weblog.rubyonrails.org/2011/2/8/new-releases-2-3-11-and-3-0-4>
- Référence CVE CVE-2011-0446 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0446>
- Référence CVE CVE-2011-0447 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0447>
- Référence CVE CVE-2011-0448 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0448>
- Référence CVE CVE-2011-0449 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0449>

## Gestion détaillée du document

10 février 2011 version initiale.