

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-2009-AVI-526>

Gestion du document

Référence	CERTA-2009-AVI-526
Titre	Vulnérabilité dans Ruby on Rails
Date de la première version	02 décembre 2009
Date de la dernière version	–
Source(s)	Annonce de mise à jour de sécurité Ruby on Rails du 30 novembre 2009
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.

2 Systèmes affectés

Ruby on Rails 2.3.x.

3 Résumé

Une vulnérabilité dans Ruby on Rails permet à un utilisateur distant malintentionné de réaliser une injection de code indirecte.

4 Description

Une vulnérabilité, causée par un manque de contrôle de la fonction `strip_tags`, peut être exploitée par une personne malveillante afin de réaliser une injection de code indirecte. Cette vulnérabilité peut être exploitée afin d'exécuter du code arbitraire dans le contexte du navigateur Internet d'un utilisateur.

5 Solution

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

6 Documentation

- Annonce de mise à jour de sécurité Ruby on Rails du 30 novembre 2009 :
<http://weblog.rubyonrails.org/2009/11/30/ruby-on-rails-2-3-5-released>

Gestion détaillée du document

02 décembre 2009 version initiale.