

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de 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-375>

Gestion du document

Référence	CERTA-2009-AVI-375
Titre	Vulnérabilité de Ruby on Rails
Date de la première version	09 septembre 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Ruby on Rails du 04 septembre 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 versions 2.0.x ;
- Ruby on Rails versions 2.1.x ;
- Ruby on Rails versions 2.2.x ;
- Ruby on Rails versions 2.3.x.

3 Résumé

Une vulnérabilité dans Ruby on Rails permet à un utilisateur distant de réaliser des attaques de type injection de code indirecte.

4 Description

Une vulnérabilité due à un manque de contrôle de certaines entrées au format unicode est présente dans l'environnement de développement Ruby on Rails. Celle-ci permet à un utilisateur distant de conduire des attaques de type injection de code indirecte.

5 Solution

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

6 Documentation

- Bulletin de sécurité Ruby on Rails du 04 septembre 2009 :
<http://weblog.rubyonrails.org/2009/9/4/xss-vulnerability-in-ruby-on-rails>
- Référence CVE CVE-2009-3009 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3009>

Gestion détaillée du document

09 septembre 2009 version initiale.