



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 22 mars 2011  
N° CERTA-2011-AVI-101-001

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans Ruby

---

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-101>

---

### Gestion du document

Référence	CERTA-2011-AVI-101-001
Titre	Multiples vulnérabilités dans Ruby
Date de la première version	22 février 2011
Date de la dernière version	22 mars 2011
Source(s)	Notes de mise à jour Ruby du 18 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.

## 2 Systèmes affectés

Pour la vulnérabilité sur la méthode `Exception#to_s` :

- Ruby versions 1.8.6 niveau de patch 420 et précédentes ;
- Ruby versions 1.8.7 niveau de patch 330 et précédentes ;
- Ruby versions de développement 1.8 (1.8.8dev).

Pour la vulnérabilité sur la méthode `FileUtils.remove_entry_secure` :

- Ruby versions 1.8.6 niveau de patch 420 et précédentes ;
- Ruby versions 1.8.7 niveau de patch 330 et précédentes ;
- Ruby versions de développement 1.8 (1.8.8dev) ;
- Ruby versions 1.9.1 niveau de patch 430 et précédentes ;
- Ruby versions 1.9.2 niveau de patch 136 et précédentes ;
- Ruby versions de développement 1.9 (1.9.3dev).

### 3 Résumé

Deux vulnérabilités dans Ruby ont été corrigées. La première permet de contourner la politique de sécurité et la seconde de porter atteinte à l'intégrité des données.

### 4 Description

La première vulnérabilité touche la méthode `to_s` de la classe `Exception`. Celle-ci permet à un attaquant de déjouer le mécanisme de sécurité permettant la séparation des données issues de sources extérieures au programme. La seconde vulnérabilité affecte la méthode `remove_entry_secure` de la classe `FileUtils`. Celle-ci cause une situation de compétition (*race condition*), qui permet à une personne malveillante d'utiliser des liens symboliques pour forcer la suppression de fichiers ou de répertoires sur le système.

### 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 Ruby du 18 février 2011 :  
<http://www.ruby-lang.org/en/news/2011/02/18/exception-methods-can-bypass-safe/>  
<http://www.ruby-lang.org/en/news/2011/02/18/fileutils-is-vulnerable-to-symlink-race-attacks/>
- Référence CVE CVE-2011-1004 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1004>
- Référence CVE CVE-2011-1005 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1005>

### Gestion détaillée du document

**22 février 2011** version initiale ;

**22 mars 2011** ajout des références CVE.