



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 12 juin 2009  
N° CERTA-2009-AVI-232

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité 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-2009-AVI-232>

---

### Gestion du document

|                             |  |
|-----------------------------|--|
| Référence                   | CERTA-2009-AVI-232                           |
| Titre                       | Vulnérabilité dans Ruby                      |
| Date de la première version | 12 juin 2009                                 |
| Date de la dernière version | –  |
| Source(s)                   | Bulletin de mise à jour Ruby du 09 juin 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

Déni de service à distance.

## 2 Systèmes affectés

Ruby versions antérieures aux versions 1.8.6-p369 et 1.8.7-p173.

## 3 Résumé

Une vulnérabilité permettant de réaliser un déni de service a été découverte dans l'interpréteur Ruby.

## 4 Description

Une vulnérabilité a été découverte dans l'interpréteur Ruby. Cette vulnérabilité résulte d'une erreur dans la bibliothèque `BigDecimal` et peut être exploitée afin de réaliser un déni de service.

## **5 Solution**

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

## **6 Documentation**

- Bulletin de mise à jour Ruby du 09 juin 2009 :  
<http://www.ruby-lang.org/en/news/2009/06/09/dos-vulnerability-in-bigdecimal/>
- Référence CVE CVE-2009-1904 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1904>

## **Gestion détaillée du document**

**12 juin 2009** version initiale.