

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-2008-AVI-402>

Gestion du document

Référence	CERTA-2008-AVI-402
Titre	Multiples vulnérabilités dans Ruby
Date de la première version	12 août 2008
Date de la dernière version	–
Source(s)	Mise à jour des versions Ruby du 08 et 11 août 2008
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

- Exécution de code arbitraire ;
- déni de service à distance ;
- élévation de privilèges.

2 Systèmes affectés

- Ruby 1.8.6 pour les versions antérieures à 1.8.6-p287 ;
- Ruby 1.8.7 pour les versions antérieures à 1.8.7-p72 ;
- Ruby 1.9 pour la version r18423 ainsi que celles antérieures.

3 Résumé

Plusieurs vulnérabilités ont été identifiées dans Ruby. Les conséquences de l'exploitation de ces dernières sont variées.

4 Description

Plusieurs vulnérabilités ont été identifiées dans Ruby :

- 1° certaines concernent les niveaux de sûreté dans Ruby, dont des méthodes comme `untrace_var()` qui ne devraient pas être autorisées à certains niveaux ou la variable `$PROGRAM_NAME` modifiable au niveau 4 ;
- 2° une mauvaise manipulation des en-têtes HTTP par WEBrick, et en particulier dans la fonction `WEBrick::HTTPUtils.split_header_value()` ;
- 3° un mauvais contrôle des appels de fonctions par la bibliothèque DL (*dynamic linker*).
- 4° une mauvaise génération d'aléas par `resolve.rb` pour les échanges DNS concernant les identifiants de transactions ou le choix des ports sources.

5 Solution

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

6 Documentation

- Annonce des vulnérabilités Ruby publiée le 08 et le 11 août 2008 :
<http://www.ruby-lang.org/en/news/2008/08/08/multiples-vulnerabilities-in-ruby/>
- Annonce des changements pour la branche 1.8 de Ruby :
<http://www.ruby-lang.org/en/news/2008/08/11/ruby-1-8-7-p72-and-1-8-6-p287-released/>
- Référence CVE CVE-2008-1447 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1447>

Gestion détaillée du document

12 août 2008 version initiale.