

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-342>

Gestion du document

Référence	CERTA-2008-AVI-342
Titre	Multiples vulnérabilités dans Ruby
Date de la première version	27 juin 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Ruby du 20 juin 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

- Atteinte à la confidentialité des données ;
- exécution de code arbitraire à distance ;
- déni de service à distance.

2 Systèmes affectés

- Ruby versions 1.8.4 et antérieures ;
- Ruby versions 1.8.5-p230 et antérieures ;
- Ruby versions 1.8.6-p229 et antérieures ;
- Ruby versions 1.8.7-p21 et antérieures ;
- Ruby versions 1.9.0-1 et antérieures.

3 Résumé

Plusieurs vulnérabilités dans Ruby permettent à un utilisateur distant de porter atteinte à la confidentialité des données, de provoquer un déni de service ou d'exécuter du code arbitraire.

4 Description

Plusieurs vulnérabilités sont présentes dans l'interpréteur Ruby ou des classes de base Ruby associées :

- la première est relative à certains composants `WEBrick` qui, sous certaines conditions, permettent à un utilisateur distant de porter atteinte à la confidentialité des données utilisées par l'application web s'appuyant sur ces composants ;
- la deuxième concerne plusieurs failles de type débordement d'entiers dans certaines fonctions de Ruby. Elle permet à un utilisateur distant de provoquer un déni de service via des paramètres de longueur excessive ;
- la dernière est due à une erreur dans certaines fonctions d'allocations de mémoire et permet à un utilisateur distant de provoquer un déni de service ou d'exécuter du code arbitraire.

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 du 20 juin 2008 :
<http://www.ruby-lang.org/en/news/2008/06/20/arbitrary-code-execution-vulnerabilities>
- Référence CVE CVE-2008-2662 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2662>
- Référence CVE CVE-2008-2663 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2663>
- Référence CVE CVE-2008-2725 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2725>
- Référence CVE CVE-2008-2726 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2726>
- Référence CVE CVE-2008-2664 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2664>

Gestion détaillée du document

27 juin 2008 version initiale.