



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 2006  
N° CERTA-2005-AVI-385-004

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de l'interpréteur de script 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-2005-AVI-385>

---

### Gestion du document

Référence	CERTA-2005-AVI-385-004
Titre	Vulnérabilité de l'interpréteur de script Ruby
Date de la première version	07 octobre 2005
Date de la dernière version	12 juin 2006
Source(s)	Bulletin de mise à jour Ruby
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 en local.

## 2 Systèmes affectés

Ruby version 1.8.2 et versions antérieures.

## 3 Description

Le mécanisme de niveau de sécurité de l'interpréteur de script Ruby est vulnérable. Un utilisateur mal-intentionné peut ainsi exécuter du code arbitraire en se dégageant de toutes les restrictions dues au mécanisme de niveau de sécurité.

## 4 Solution

La version 1.8.3 corrige cette vulnérabilité. Pour mettre à jour, consulter le site de l'éditeur (cf. Documentation).  
Sous *Gentoo*, utiliser *emerge* comme suit :

```
# emerge --sync  
# emerge --ask --oneshot --verbose `>=dev-lang/ruby-1.8.3`
```

## 5 Documentation

- Bulletin de l'éditeur :  
<http://www.ruby-lang.org/en/20051003.html>
- Bulletin de sécurité Gentoo GLSA 200510-05 du 06 octobre 2005 :  
<http://security.gentoo.org/glsa/glsa-200510-05.xml>
- Bulletin de sécurité RedHat RHSA-2005-799 du 11 octobre 2005 :  
<http://rhn.redhat.com/errata/RHSA-2005-799.html>
- Bulletin de sécurité Mandriva MDKSA-2006:079 du 25 avril 2006 :  
<http://wwwnew.mandriva.com/security/advisories?name=MDKSA-2006:079>
- Bulletin de sécurité Debian DSA-860 du 11 octobre 2005 :  
<http://www.debian.org/security/2005/dsa-860>
- Bulletin de sécurité Debian DSA-862 du 11 octobre 2005 :  
<http://www.debian.org/security/2005/dsa-862>
- Bulletin de sécurité Debian DSA-864 du 13 octobre 2005 :  
<http://www.debian.org/security/2005/dsa-864>
- Bulletin de sécurité Ubuntu USN-195-1 du 10 octobre 2005 :  
<http://www.ubuntu.com/usn/usn-195-1>
- Bulletin de sécurité Ubuntu USN-273-1 du 24 avril 2006 :  
<http://www.ubuntu.com/usn/usn-273-1>
- Bulletin de sécurité RedHat RHSA-2006-0427 du 09 mai 2006 :  
<https://rhn.redhat.com/errata/RHSA-2006-0427.html>
- Référence CVE CAN-2005-2337 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2337>
- Référence CVE CAN-2006-1931 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-1931>

### Gestion détaillée du document

**07 octobre 2005** version initiale.

**12 octobre 2005** ajout des références aux bulletins de sécurité des éditeurs.

**14 octobre 2005** ajout de la référence au bulletin de sécurité Debian et référence CVE.

**27 avril 2006** ajout des références aux bulletins de sécurité Mandriva, Ubuntu et de la référence CVE.

**12 juin 2006** ajout de la référence au bulletin de sécurité RedHat.