

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : 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-2006-AVI-562>

Gestion du document

Référence	CERTA-2006-AVI-562-001
Titre	Vulnérabilités dans Ruby
Date de la première version	18 décembre 2006
Date de la dernière version	26 mars 2007
Source(s)	Mise à jour de sécurité Ruby en version 1.8.5-p2
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 1.8.5 et versions antérieures.

3 Résumé

Deux vulnérabilités dans Ruby permettent à un utilisateur distant malintentionné de provoquer un déni de service.

4 Description

Ruby est un langage interprété orienté objet.

Deux vulnérabilités découvertes dans le fichier `cgi.rb` permettent à un utilisateur malintentionné de provoquer un déni de service à distance au moyen de requêtes HTTP spécialement construites. Le déni de service se traduit par une consommation excessive du temps processeur.

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 04 décembre 2006 :
<http://www.ruby-lang.org/en/news/2006/12/04/another-dos-vulnerability-in-cgi-library/>
- Bulletin de sécurité Debian DSA-1234 du 13 décembre 2006 :
<http://www.debian.org/security/2006/dsa-1234>
- Bulletin de sécurité Debian DSA-1235 du 13 décembre 2006 :
<http://www.debian.org/security/2006/dsa-1235>
- Bulletin de sécurité Gentoo GLSA-200611-12 du 20 novembre 2006 :
<http://www.gentoo.org/security/en/glsa/glsa-200611-12.xml>
- Bulletin de sécurité Gentoo GLSA-200612-21 du 20 décembre 2006 :
<http://www.gentoo.org/security/en/glsa/glsa-200612-21.xml>
- Bulletin de sécurité Mandriva MDKSA-2006:192 du 27 octobre 2006 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2006:192>
- Bulletin de sécurité Mandriva MDKSA-2006:225 du 06 décembre 2006 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2006:225>
- Bulletin de sécurité Ubuntu USN-371-1 du 31 octobre 2006 :
<http://www.ubuntu.com/usn/usn-371-1>
- Bulletin de sécurité Ubuntu USN-394-1 du 08 décembre 2006 :
<http://www.ubuntu.com/usn/usn-394-1>
- Bulletin de sécurité Red Hat RHSA-2006:0729 du 08 novembre 2006 :
<http://rhn.redhat.com/errata/RHSA-2006-0729.html>
- Bulletin de sécurité SuSE SUSE-SR:2006:026 du 17 novembre 2006 :
<http://lists.suse.com/archive/suse-security-announce/2006-Nov/0008.html>
- Bulletin de sécurité SuSE SUSE-SR:2007:004 du 16 mars 2006 :
<http://lists.suse.com/archive/suse-security-announce/2007-Mar/0005.html>
- Référence CVE CVE-2006-5467 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5467>
- Référence CVE CVE-2006-6303 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6303>

Gestion détaillée du document

18 décembre 2006 version initiale.

26 mars 2007 ajout des références aux bulletins de sécurité Gentoo et Suse.