

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Ruby on Rails

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-2011-AVI-459>

Gestion du document

Référence	CERTA-2011-AVI-459-003
Titre	Multiples vulnérabilités dans Ruby on Rails
Date de la première version	18 août 2011
Date de la dernière version	16 septembre 2011
Sources	Annonces de mises à jour de sécurité de Ruby on Rails du 16 août 2011
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

- Contournement de la politique de sécurité ;
- atteinte à l'intégrité des données ;
- injection de code indirecte à distance.

2 Systèmes affectés

- Ruby on Rails 2.3.x ;
- Ruby on Rails 3.0.x.

3 Résumé

De multiples vulnérabilités présentes dans le produit *Ruby on Rails* ont été corrigées. Elles permettent le contournement de la politique de sécurité, l'injection de code SQL et l'injection de code HTML dans une réponse.

4 Description

De multiples vulnérabilités présentes dans le produit *Ruby on Rails* ont été corrigées. Ces vulnérabilités permettent notamment :

- le rendu de vues de données normalement inaccessibles à l'utilisateur ;
- l'injection de code dans les requêtes SQL ;
- l'injection de code javascript dans les réponses HTML ;
- l'envoi de chaînes Unicode malformées dans les réponses HTML.

5 Solution

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

Note : une mise à jour pour la version 3.1 RC est également disponible.

6 Documentation

- Annonce de publication Ruby on Rails 2.3.14 :
<http://weblog.rubyonrails.org/2011/8/16/ann-rails-2-3-14>
- Annonce de publication Ruby on Rails 3.0.10 :
<http://weblog.rubyonrails.org/2011/8/16/ann-rails-3-0-10>
- Secunia Advisory SA45648 :
<http://secunia.com/advisories/45648/>
- Bulletin de sécurité Debian DSA 2301-1 du 5 septembre 2011 :
<http://www.debian.org/security/2011/dsa-2301>
- Bulletin de sécurité Fedora FEDORA-2011-11567 du 7 septembre 2011 :
<http://lists.fedoraproject.org/pipemail/package-announce/2011-Septembre/065137.html>
- Référence CVE CVE-2011-292
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2929>
- Référence CVE CVE-2011-2930
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2930>
- Référence CVE CVE-2011-2931
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2931>
- Référence CVE CVE-2011-2932
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2932>
- Référence CVE CVE-2011-3186
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3186>

Gestion détaillée du document

18 août 2011 version initiale.

23 août 2011 ajout des références CVE.

14 septembre 2011 ajout des références aux bulletins Debian et Fedora.

16 septembre 2011 ajout d'une référence CVE.