

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le module Safe de Perl

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-2010-AVI-580>

Gestion du document

Référence	CERTA-2010-AVI-580
Titre	Vulnérabilité dans le module Safe de Perl
Date de la première version	07 décembre 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Oracle Sun Solaris CVE_2010_1168 du 26 novembre 2010
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 à distance.

2 Systèmes affectés

Module Perl Safe, version 2.24 et versions antérieures.

3 Résumé

Une vulnérabilité dans le module Safe de Perl permet à un utilisateur malveillant d'exécuter du code arbitraire à distance.

4 Description

Un attaquant peut contourner les restrictions de `Safe::reval` et de `Safe::rdo` et exécuter du code arbitraire à distance.

5 Solution

La version 2.25 et les versions suivantes du module Safe remédient à ce problème.
Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Site de téléchargement du projet Perl :
<http://www.perl.org/>
- Bulletin de sécurité Mandriva MDVSA-2010:115 du 11 juin 2010 :
<http://www.mandriva.com/security/advisories?name=MDVSA-2010:115>
- Bulletin de sécurité Mandriva MDVSA-2010:116 du 11 juin 2010 :
<http://www.mandriva.com/security/advisories?name=MDVSA-2010:116>
- Bulletin de sécurité Oracle Sun Solaris CVE_2010_1168 du 26 novembre 2010 :
http://blogs.sun.com/security/entry/cve_2010_1168_vulnerability_in
- Bulletin de sécurité RedHat RHSA-2010:0457 du 07 juin 2010 :
<http://rhn.redhat.com/errata/RHSA-2010-0457.html>
- Bulletin de sécurité RedHat RHSA-2010:0458 du 07 juin 2010 :
<http://rhn.redhat.com/errata/RHSA-2010-0458.html>
- Référence CVE CVE-2010-1168 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1168>

Gestion détaillée du document

07 décembre 2010 version initiale.