Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S.G.D.S.N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 29 mai 2007
N° CERTA-2007-AVI-151-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité mod_perl pour Apache

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-2007-AVI-151`

Gestion du document

Référence	CERTA-2007-AVI-151-001
Titre	Vulnérabilité mod_perl pour Apache
Date de la première version	03 avril 2007
Date de la dernière version	29 mai 2007
Source(s)	Note de changement de la version 1.30 du 29 mars 2007 Alerte TA05-023A de l'US-CERT
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

– `mod_perl`, pour les versions antérieures à 1.30.

3 Description

Une vulnérabilité a été identifiée dans `mod_perl`, le module d'interprétation Perl d'Apache. Les fichiers `PerlRun.pm` et `RegistryCooker.pm` comporteraient une erreur lors de la manipulation d'une `URI` (pour *Uniform Resource Identifier*) par une expression régulière.

Une personne malveillante pourrait donc exploiter cette vulnérabilité à distance, par le biais d'une `URI` spécialement construite, afin de perturber le système vulnérable.

4 Solution

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

5 Documentation

- RFC 3986, "Uniform Resource Identifier (URI): Generic Syntax :
  http://www.ietf.org/rfc/rfc3986.txt
- Page du projet `mod_perl` pour Apache :
  http://perl.apache.org
- Notes de changement pour la version 1.30 de `mod_perl` :
  http://svn.apache.org/repos/asf/perl/modperl/branches/1.x/Changes
- Bulletin de sécurité SuSE SUSE-SR:2007:012 :
  http://lists.suse.com/archive/suse-security-announce/2007-May/0008.html
- Référence CVE CVE-2007-1349 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1349

Gestion détaillée du document

03 avril 2007 version initiale.

29 mai 2007 ajout de la référence au bulletin de sécurité SuSE.