

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans 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-2009-AVI-149>

Gestion du document

Référence	CERTA-2009-AVI-149-001
Titre	Vulnérabilité dans mod_perl pour Apache
Date de la première version	17 avril 2009
Date de la dernière version	17 décembre 2009
Source(s)	Note de changements de la version 1.31 du 01 avril 2009
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

Injection de code indirecte.

2 Systèmes affectés

– mod_perl, pour les versions antérieures à 1.31.

3 Résumé

Une vulnérabilité dans le module mod_perl pour Apache permet à une personne distante malintentionnée de réaliser une injection de code indirecte (*cross site scripting*).

4 Description

Une vulnérabilité causée par un manque de contrôle des variables fournies aux modules Apache::Status et Apache2::Status permet à une personne malveillante d'injecter du code arbitraire dans le contexte du navigateur Internet d'un utilisateur.

5 Solution

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

6 Documentation

- Page du projet `mod_perl` pour Apache :
<http://perl.apache.org>
- Notes de changements pour la version 1.31 de `mod_perl` :
<http://svn.apache.org/repos/asf/perl/modperl/branches/1.x/Changes>
- Bulletin de sécurité Mandriva MDVSA-2009:091 du 12 avril 2009 :
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:091>
- Bulletin de sécurité Sun Solaris #274110 du 15 décembre 2009 :
<http://sunsolve.sun.com/search/document.do?assetkey=1-66-274110-1>
- Référence CVE CVE-2009-0796 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0796>

Gestion détaillée du document

17 avril 2009 version initiale ;

17 décembre 2009 ajout des bulletins de sécurité Sun Solaris et Mandriva.