

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du module `mod_survey`

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-2004-AVI-101>

Gestion du document

Référence	CERTA-2004-AVI-101
Titre	Vulnérabilité du module <code>mod_survey</code>
Date de la première version	25 mars 2004
Date de la dernière version	–
Source(s)	Avis de sécurité de <code>mod_survey</code> du 21 mars 2004
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.

2 Systèmes affectés

- Module `mod_survey` versions 3.0.16-pre1 et antérieures (branche stable) ;
- module `mod_survey` versions 3.2.0-pre3 et antérieures (branche de développement) ;

3 Résumé

Un utilisateur mal intentionné peut exploiter une vulnérabilité du module `mod_survey` pour exécuter du code arbitraire.

4 Description

Le module `mod_survey` est un module du serveur HTTP Apache, utilisé pour traiter des questionnaires au format XML.

Il n'est pas installé par défaut.

Une vulnérabilité a été découverte dans le traitement des données. Elle permet d'injecter du code malicieux dans le rapport généré par le module *mod_survey*.

Cette vulnérabilité peut être exploitée par un utilisateur distant mal intentionné pour exécuter du code arbitraire.

5 Solution

Mettre à jour le module *mod_survey*. Les versions suivantes corrigent cette vulnérabilité :

- branche stable : version 3.0.16-pre2 ;
- branche de développement : version 3.2.0-pre4.

6 Documentation

- Avis de sécurité de *mod_survey* du 21 mars 2004 :
<http://gathering.itm.mh.se/modsurvey/SA20040321.txt>
- Note d'information du CERTA sur les vulnérabilités de type "Cross Site Scripting" :
<http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-001/index.html>

Gestion détaillée du document

25 mars 2004 version initiale.