

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Mambo

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-566>

Gestion du document

Référence	CERTA-2007-AVI-566
Titre	Multiples vulnérabilités dans Mambo
Date de la première version	27 décembre 2007
Date de la dernière version	–
Source(s)	Annonce de la publication Mambo version 4.6.3 du 24 décembre 2007
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 ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- les versions de Mambo antérieures à 4.6.3.

3 Résumé

Plusieurs vulnérabilités ont été identifiées dans le gestionnaire de contenus Mambo. L'exploitation de ces dernières par le biais de pages web spécialement construites peut conduire à l'exécution de code arbitraire sur le système vulnérable.

4 Description

Plusieurs vulnérabilités ont été identifiées dans le gestionnaire de contenus Mambo. L'une d'elles est similaire à celle mentionnée dans l'avis CERTA-2007-AVI-274 concernant PHPMailer. D'autres sont des vulnérabilités permettant d'effectuer des injections indirectes de code (XSS).

L'exploitation de plusieurs de ces vulnérabilités par le biais de pages web spécialement construites peut conduire à l'exécution de code arbitraire sur le système vulnérable.

5 Solution

Se référer à la mise à jour du projet Mambo pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Site officiel du projet Mambo, et annonce de la version 4.6.3 du 24 décembre 2007 :
<http://source.mambo-foundation.org>
- Document du CERTA CERTA-2007-AVI-274 du 20 juin 2007 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-274/index.html>
- Référence CVE CVE-2007-3215 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3215>

Gestion détaillée du document

27 décembre 2007 version initiale.