

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : 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-2008-AVI-280>

Gestion du document

Référence	CERTA-2008-AVI-280
Titre	Vulnérabilités dans Mambo
Date de la première version	29 mai 2008
Date de la dernière version	–
Source(s)	Annonce de la version 4.6.4 de Mambo du 24 mai 2008
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 SQL ;
- injections de code indirectes (*cross-site scripting*).

2 Systèmes affectés

Mambo versions 4.6.3 et antérieures.

3 Résumé

Plusieurs vulnérabilités affectant *Mambo* permettent de réaliser diverses injections.

4 Description

Trois vulnérabilités ont été découvertes dans *Mambo* :

- une injection de code SQL est possible via les paramètres `articleid` et `mcname` du fichier `index.php`. L'exploitation de cette vulnérabilité n'est possible que si la fonctionnalité `magic_quotes_gpc` est désactivée dans le fichier de configuration de PHP ;

- les entêtes HTTP des réponses envoyées par le serveur peuvent être manipulées ;
- des attaques de type *cross-site scripting* sont possibles dans *MOSTlyCE* (versions 3.0 et antérieures). La versions 4.6.4 de *Mambo* inclut *MOSTlyCE* version 3.05.

5 Solution

Mettre *Mambo* à jour en version 4.6.4 (cf. section Documentation).

6 Documentation

- Site de téléchargement de *Mambo* version 4.6.4 :
<http://mambo-code.org/gf/project/mambo/frs/>
- Annonce de la version 4.6.4 de *Mambo* du 24 mai 2008 :
<http://forum.mambo-foundation.org/showthread.php?t=11799>
- Référence CVE-2008-2497 :
<http://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-2497>
- Référence CVE-2008-2498 :
<http://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-2498>

Gestion détaillée du document

29 mai 2008 version initiale.