

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans Microsoft Content Manager Server 2001

---

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-2002-AVI-168>

---

### Gestion du document

Référence	CERTA-2002-AVI-168
Titre	Vulnérabilités dans Microsoft Content Manager Server 2001
Date de la première version	08 août 2002
Date de la dernière version	–
Source(s)	Bulletin Microsoft MS02-041
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 ;
- élévation de privilèges ;
- déni de service.

## 2 Systèmes affectés

Microsoft Content Management Server 2001.

## 3 Résumé

Microsoft Content Management Server 2001 (MCMS) est un produit simplifiant le développement et la gestion des sites internet de commerce électronique.

Trois vulnérabilités ont été découvertes, permettant à un utilisateur distant mal intentionné, de réaliser une augmentation de privilèges sur le serveur, d'exécuter du code arbitraire ou d'entraîner un déni de service sur la machine cible.

## 4 Description

- Première vulnérabilité :  
Un débordement de mémoire dans une fonction d'authentification permet à un utilisateur distant de réaliser un déni de service ou d'exécuter du code arbitraire avec les privilèges `system`.
- Seconde vulnérabilité :  
MCMS comporte une fonctionnalité permettant à des utilisateurs authentifiés de mettre en place, à distance, des pages sur le serveur.  
Une vulnérabilité dans le contrôle de l'authentification permet à un utilisateur de contourner cette authentification et de pouvoir placer des documents sur le serveur. De plus une autre vulnérabilité permet également de choisir l'emplacement du fichier à mettre en place, permettant ainsi à un utilisateur mal intentionné de pouvoir placer tout type de fichier dans l'arborescence du serveur. Ce fichier pourrait ensuite être exécuter avec les droits d'utilisateur non privilégié.
- Troisième vulnérabilité :  
Une fonctionnalité permet à tout utilisateur de consulter par le biais d'une requête sur une base de données SQL les fichiers disponibles sur le serveur.  
Une vulnérabilité dans le contrôle de la requête SQL permet, à un utilisateur distant, d'exécuter n'importe quelle action sur la base de données ou de diriger des commandes vers le système d'exploitation.

## 5 Solution

Télécharger le correctif disponible sur le site Microsoft :  
<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=41266>

## 6 Documentation

Bulletin Microsoft :  
<http://www.microsoft.com/technet/security/bulletin/MS02-041.asp>

## Gestion détaillée du document

**08 août 2002** version initiale.