

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Microsoft Content Management Server (CMS)

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-165>

Gestion du document

Référence	CERTA-2007-AVI-165-001
Titre	Vulnérabilités dans Microsoft Content Management Server (CMS)
Date de la première version	11 avril 2007
Date de la dernière version	13 juin 2007
Source(s)	Bulletin de sécurité Microsoft MS07-018 du 10 avril 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

- Microsoft Content Management Server (CMS) 2001 Service Pack 1 ;
- Microsoft Content Management Server (CMS) 2002 Service Pack 2.

3 Résumé

Deux vulnérabilités ont été identifiées dans Microsoft Content Management Server (CMS). Exploitées par une personne, celles-ci permettraient l'exécution de code arbitraire à distance sur le système vulnérable ou le contournement de la politique de sécurité (accès illégitime aux données de l'utilisateur, modification des caches de navigation, etc.).

4 Description

Deux vulnérabilités ont été identifiées dans Microsoft Content Management Server (CMS), un outil permettant de créer et maintenir du contenu de sites Web :

- 1° la première serait due à une mauvaise manipulation d'adresses réticulaires (ou URLs) se trouvant dans les requêtes HTTP pour le CMS. Une personne malveillante pourrait construire un paquet particulier, et l'envoyer vers la machine vulnérable, afin d'en prendre le contrôle complet à distance.
- 2° la seconde consisterait en une vérification incorrecte des entrées fournies par une requête de redirection HTML adressée au client. Une personne malveillante pourrait exploiter cette vulnérabilité pour faire une injection de code indirecte (*cross site scripting*), ce qui lui permettrait de contourner la politique de sécurité (accès illégitime aux données de l'utilisateur, modification des caches de navigation, etc.).

5 Solution

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

6 Documentation

- Bulletin de sécurité Microsoft MS07-018 du 10 avril 2007, mis à jour le 12 juin 2007 :
<http://www.microsoft.com/france/technet/security/bulletin/MS07-018.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS07-018.msp>
- Référence CVE CVE-2007-0938 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0938>
- Référence CVE CVE-2007-0939 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0939>

Gestion détaillée du document

11 avril 2007 version initiale;

13 juin 2007 mise à jour du bulletin MS07-018 le 12 juin 2007 par l'éditeur.