

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Open Web Access

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-355>

Gestion du document

Référence	CERTA-2008-AVI-355
Titre	Vulnérabilités dans Open Web Access
Date de la première version	09 juillet 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS08-039 du 08 juillet 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

Élévation de privilèges.

2 Systèmes affectés

- *Microsoft Exchange Server 2003 SP2* ;
- *Microsoft Exchange Server 2007* ;
- *Microsoft Exchange Server 2007 SP1*.

3 Résumé

Deux vulnérabilités dans *Open Web Access for Microsoft Exchange* permettent à un utilisateur malveillant d'élever ses privilèges.

4 Description

Une première vulnérabilité, de type injection de code indirecte (*cross site scripting*), repose sur un défaut de validation des données entrées par l'utilisateur. Son exploitation permet à un utilisateur malveillant d'exécuter des commandes avec les droits d'un autre utilisateur.

Une deuxième vulnérabilité, également de type injection de code indirecte (*cross site scripting*), provient d'un défaut dans le traitement du langage HTML. Son exploitation permet à un utilisateur malveillant d'exécuter des commandes avec les droits d'un autre utilisateur.

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 MS08-039 du 08 juillet 2008 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS08-039.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS08-039.msp>
- Référence CVE CVE-2008-2247 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2247>
- Référence CVE CVE-2008-2248 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2248>

Gestion détaillée du document

09 juillet 2008 version initiale.