

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Microsoft Exchange Server Outlook 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-2003-AVI-172>

Gestion du document

Référence	CERTA-2003-AVI-172
Titre	Vulnérabilité de Microsoft Exchange Server Outlook Web Access
Date de la première version	16 octobre 2003
Date de la dernière version	-
Source(s)	Avis de sécurité Microsoft MS03-047
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

Attaques de type "Cross Site Scripting".

2 Systèmes affectés

Microsoft Exchange Server 5.5 SP4.

Les serveurs Microsoft Exchange 2000 Server et Microsoft Exchange Server 2003 ne sont pas vulnérables.

3 Résumé

Une vulnérabilité de Microsoft Exchange Outlook Web Access (OWA) permet à un utilisateur mal intentionné de provoquer une attaque de type "Cross Site Scripting".

4 Description

Outlook Web Access ne gère pas correctement le code HTML lors de la création d'un nouveau message et permet ainsi les attaques de type "Cross Site Scripting".

Il est possible pour un utilisateur mal intentionné d'envoyer à une victime utilisant OWA un message contenant un script qui s'exécutera avec les privilèges de la victime.

5 Solution

Appliquer le correctif proposé par Microsoft (cf. section Documentation).

6 Documentation

Avis de sécurité Microsoft :

<http://www.microsoft.com/technet/security/bulletin/MS03-047.asp>

Référence CVE CAN-2003-0712 :

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0712>

Note d'information du CERTA CERTA-2002-INF-001 sur les vulnérabilité de type "Cross Site Scripting" :

<http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-001/index.html>

Gestion détaillée du document

16 octobre 2003 version initiale.