

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Microsoft Outlook Express

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-080>

Gestion du document

Référence	CERTA-2003-AVI-080
Titre	Vulnérabilité dans Microsoft Outlook Express
Date de la première version	28 avril 2003
Date de la dernière version	–
Source(s)	Bulletin de sécurité MS03-014 de Microsoft
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 scripts à distance.

2 Systèmes affectés

- Microsoft Outlook Express 5.5 ;
- Microsoft Outlook Express 6.0.

3 Résumé

Une vulnérabilité présente dans le client de messagerie Outlook Express permet d'exécuter des scripts sur le poste de l'utilisateur.

4 Description

MHTML (MIME Encapsulation of Aggregate HTML) permet l'envoi de documents HTML dans des messages électroniques. Sur la plate-forme Windows, le traitement d'un lien hypertexte (url) MHTML est réalisé par Outlook Express.

Un utilisateur mal intentionné peut, au moyen d'un message électronique ou d'une page HTML habilement constitué, exploiter la vulnérabilité présente dans le traitement des urls MHTML pour réaliser l'exécution d'un script sur le poste de l'utilisateur employant une version vulnérable d'Outlook Express.

5 Solution

Appliquer le correctif de l'éditeur (cf. section Documentation).

6 Documentation

- Bulletin de sécurité MS03-14 de Microsoft :
<http://www.microsoft.com/technet/security/bulletin/MS03-014.mspx>
- Référence CVE CAN-2002-0980 :
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0980>

Gestion détaillée du document

28 avril 2003 version initiale.