

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans 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-2004-AVI-128>

Gestion du document

Référence	CERTA-2004-AVI-128
Titre	Vulnérabilité dans Outlook Express
Date de la première version	14 avril 2004
Date de la dernière version	–
Source(s)	Avis de sécurité Microsoft MS04-O13
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.

2 Systèmes affectés

- Microsoft Outlook Express 5.5 SP2 ;
- Microsoft Outlook Express 6 ;
- Microsoft Outlook Express 6 SP1 ;
- Microsoft Outlook Express 6 SP1 (64 bits) ;
- Microsoft Outlook Express 6 sur Windows Server 2003 ;
- Microsoft Outlook Express 6 sur Windows Server 2003 (64 bits).

3 Résumé

Une vulnérabilité présente dans Outlook Express permet à un utilisateur malicieux d'exécuter du code arbitraire sur la machine vulnérable.

4 Description

MHTML est le format MIME Encapsulation of Aggregate HTML Documents qui définit la structure MIME permettant d'envoyer un document HTML dans un message électronique.

Une vulnérabilité dans la gestion des pages MHTML permet à un utilisateur mal intentionné, via un courrier électronique ou une page web, d'exécuter du code arbitraire dans la zone de sécurité de la machine locale avec les privilèges de l'utilisateur connecté.

5 Contournement provisoire

Configurer Outlook Express pour une lecture des messages électroniques au format texte.

6 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs :
<http://www.microsoft.com/technet/security/bulletin/ms04-013.msp>

7 Documentation

Référence CVE CAN-2004-0380 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0380>

Gestion détaillée du document

14 avril 2004 version initiale.