

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-2006-AVI-149>

Gestion du document

Référence	CERTA-2006-AVI-149
Titre	Vulnérabilité dans Microsoft Outlook Express
Date de la première version	12 avril 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité MS06-016 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 code arbitraire à distance.

2 Systèmes affectés

- Microsoft Outlook Express 5.5 Service Pack 2 pour Microsoft Windows 2000 Service Pack 4 ;
- Microsoft Outlook Express 6 Service Pack 1 pour Microsoft Windows 2000 Service Pack 4 ou Windows XP Service Pack 1 ;
- Microsoft Outlook Express 6 pour Microsoft Windows XP Service Pack 2 (incluant la version 64-bit Edition) ;
- Microsoft Outlook Express 6 pour Microsoft Windows Server 2003 ou pour Windows Server 2003 Service Pack 1 (incluant la version 64-bit Edition).

3 Résumé

Une vulnérabilité dans Microsoft Outlook Express peut être utilisée par un utilisateur malveillant pour exécuter du code arbitraire à distance.

4 Description

L'application de messagerie Microsoft Outlook Express ne manipule pas correctement les fichiers dédiés au carnet d'adresse, au format .wab (pour *Windows Address Book*). Un utilisateur malveillant peut conduire l'utilisateur à manipuler de tels fichiers (envoi en pièce jointe d'un courriel par exemple), et profiter de cette vulnérabilité pour exécuter du code arbitraire à distance.

5 Solution

Appliquer le correctif tel qu'indiqué dans le bulletin de sécurité Microsoft MS06-016 (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS06-016 du 11 avril 2006 :
<http://www.microsoft.com/france/technet/securite/MS06-016.mspx>
<http://www.microsoft.com/technet/security/Bulletin/MS06-016.mspx>
- Référence CVE CVE-2006-0014 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0014>

Gestion détaillée du document

12 avril 2006 version initiale.