



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité
des systèmes d'information
CERTA

Paris, le 13 décembre 2006
N° CERTA-2006-AVI-548

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-548>

Gestion du document

Référence	CERTA-2006-AVI-548
Titre	Vulnérabilité dans Microsoft Outlook Express
Date de la première version	13 décembre 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS06-076 du 12 décembre 2006
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 Windows 2000 Service Pack 4 ;
- Microsoft Windows XP Service Pack 2 ;
- Microsoft Windows XP Professionnel Édition x64 ;
- Microsoft Windows Serveur 2003 (incluant les systèmes Itanium) ;
- Microsoft Windows Serveur 2003 Service Pack 1 (incluant les systèmes Itanium) ;
- Microsoft Windows Serveur 2003 Édition x64.

3 Résumé

Une vulnérabilité dans Microsoft Outlook Express permet à un utilisateur distant malintentionné d'exécuter du code arbitraire à distance.

4 Description

Une vulnérabilité de type débordement de mémoire dans Windows Address Book mise en œuvre dans Microsoft Outlook Express peut être exploitée par un utilisateur malveillant afin d'exécuter du code arbitraire à distance au moyen d'un fichier wab spécialement construit.

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 MS06-076 du 12 décembre 2006 :
<http://www.microsoft.com/france/technet/security/bulletin/MS06-076.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS06-076.msp>
- Référence CVE CVE-2006-2386 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2386>

Gestion détaillée du document

13 décembre 2006 version initiale.