

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités de Microsoft Outlook

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-2007-AVI-017>

Gestion du document

Référence	CERTA-2007-AVI-017
Titre	Vulnérabilités de Microsoft Outlook
Date de la première version	09 janvier 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS07-003 du 09 janvier 2007
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 Office 2000 Service Pack 3 : Microsoft Outlook 2000 ;
- Microsoft Office XP Service Pack 3 : Microsoft Outlook 2002 ;
- Microsoft Office 2003 Service Pack 2 : Microsoft Outlook 2003.

3 Résumé

Des vulnérabilités ont été identifiées dans Microsoft Outlook. Elles permettraient à une personne malveillante qui exploiterait l'une d'elles, de prendre le contrôle de la machine ayant une version d'Outlook vulnérable.

4 Description

Des vulnérabilités ont été identifiées dans Microsoft Outlook. Parmi celles-ci :

- Outlook ne gère pas correctement certaines informations contenues dans les en-têtes de courriels. Une personne pourrait envoyer un courriel construit avec une en-tête particulière, afin de perturber le client de messagerie Outlook qui chercherait à réceptionner le message.
- Outlook ne manipulerait pas correctement les fichiers contenant un enregistrement VEVENT. Cet enregistrement est issu du standard iCalendar (RFC 2445) pour des échanges de données liées au calendrier : il décrit un évènement dans une fenêtre de temps donné. Cette vulnérabilité permettrait à une personne malveillante envoyant un fichier iCalendar (.ICS) exploitant celle-ci d'exécuter des commandes arbitraires à distance, avec les droits de l'utilisateur local.
- Outlook ne manipulerait pas correctement les fichiers au format .oss (pour *Office Saved Searches*) associés à la fonction Recherche avancée. Ils sont utilisés dans le cas de sauvegardes des résultats de recherches (menu "Fichier", option "Enregistrer la recherche en tant que dossier de recherche"). Une personne malveillante pourrait envoyer un courriel contenant en pièce jointe un document .oss spécialement conçu. Le fait d'ouvrir cette pièce jointe provoquerait alors l'exécution de code arbitraire sur la machine ayant une version d'Outlook vulnérable.

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 MS07-003 du 09 janvier 2007 :
<http://www.microsoft.com/france/technet/security/bulletin/MS07-003.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS07-003.msp>
- Référence CVE CVE-2006-1305 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1305>
- Référence CVE CVE-2007-0033 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0033>
- Référence CVE CVE-2007-0034 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0034>

Gestion détaillée du document

09 janvier 2007 version initiale.