

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : VULnérabilité dans Microsoft Outlook Express et Windows Mail

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-431>

Gestion du document

Référence	CERTA-2007-AVI-431
Titre	VULnérabilité dans Microsoft Outlook Express et Windows Mail
Date de la première version	10 octobre 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS07-056 du 09 octobre 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 ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- Microsoft Outlook Express 6 ;
- Microsoft Outlook Express 6 Service Pack 1 ;
- Microsoft Outlook Express 5.5 Service Pack 2 ;
- Windows Mail (Vista).

Cela concerne donc les versions Outlook Express 6 (Service Pack 1 inclus).

3 Résumé

Une vulnérabilité a été identifiée dans les clients de messagerie Microsoft Outlook Express et Windows Mail. Elle concerne l'interprétation de trames du protocole NNTP. L'exploitation de cette dernière, à distance et par le biais de paquets spécialement construits, peut provoquer l'exécution de code arbitraire sur le système vulnérable.

4 Description

Une vulnérabilité a été identifiée dans les clients de messagerie Microsoft Outlook Express et Windows Mail. Elle concerne l'interprétation de trames du protocole NNTP (pour *Network News Transfer Protocol*). Ce dernier est utilisé pour échanger des informations de type *news*. Il a été initialement présenté dans le standard RFC 977 (1986), lui-même remplacé par le plus récent RFC 3977 (2006). Les ports TCP couramment utilisés pour les échanges de données sont 119/TCP et 563/TCP (NNTPS).

L'exploitation de cette vulnérabilité, à distance et par le biais de paquets spécialement construits, peut provoquer l'exécution de code arbitraire sur le système vulnérable.

5 Solution

Se référer au bulletin de sécurité MS07-056 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS07-056 du 09 octobre 2007 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS07-056.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS07-056.msp>
- Référence CVE CVE-2007-3897 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3897>
- RFC 3977, "Network News Transfer Protocol (NNTP)", October 2006 :
<http://tools.ietf.org/rfc/rfc3977.txt>
- RFC 977, "Network News Transfer Protocol, A Proposed Standard for the Stream-Based Transmission of News", February 2006 :
<http://tools.ietf.org/rfc/rfc977.txt>

Gestion détaillée du document

10 octobre 2007 version initiale.