

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-2005-AVI-210>

---

### Gestion du document

Référence	CERTA-2005-AVI-210
Titre	Vulnérabilité dans Microsoft Outlook Express
Date de la première version	15 juin 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité MS05-030 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 200 ;
- Microsoft Outlook Express 6 Service Pack 1 pour Microsoft Windows 2000 et Microsoft Windows XP ;
- Microsoft Outlook Express 6 Service Pack 1 pour Microsoft Windows 64 bit Edition ;
- Microsoft Outlook Express 6 Service pour Microsoft Windows 64 bit Edition (Itanium) ;
- Microsoft Outlook Express 6 pour Windows 2003 Server et Windows 2003 Server (Itanium).

## 3 Description

Selon Microsoft, une vulnérabilité est présente dans Microsoft Outlook Express lors de l'interprétation des réponses d'un serveur de Newsgroups (protocole nntp).

Lors de l'accès à un serveur de Newsgroups malicieusement constitué, cette vulnérabilité peut être exploitée pour exécuter du code arbitraire à distance sur la plate-forme client utilisant une version vulnérable du logiciel Microsoft Outlook Express.

## **4 Contournement provisoire**

Dans l'attente de l'application du correctif, filtrer l'accès aux ports 119/TCP et 119/UDP utilisés par le protocole nntp.

## **5 Solution**

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs.

## **6 Documentation**

- Bulletin de sécurité de Microsoft MS05-030 du 14 juin 2005 :  
<http://www.microsoft.com/technet/security/Bulletin/MS05-030.mpx>
- Référence CVE CAN-2005-1213 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1213>

## **Gestion détaillée du document**

**15 juin 2005** version initiale.