

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-2002-AVI-223>

---

### Gestion du document

Référence	CERTA-2002-AVI-223
Titre	Vulnérabilité dans Microsoft Outlook Express
Date de la première version	11 octobre 2002
Date de la dernière version	–
Source(s)	Bulletin Microsoft MS02-058
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.

## 2 Systèmes affectés

- Microsoft Outlook Express 5.5 ;
- Microsoft Outlook Express 6.0.

## 3 Résumé

Une vulnérabilité dans la gestion des signatures numériques de courrier par Microsoft Outlook Express permet à un utilisateur distant d'exécuter du code arbitraire sur la machine cible.

## 4 Description

Lors de la réception d'un mél signé de type S/MIME, Outlook Express analyse la signature et fournit un message d'erreur en cas de problème sur celle-ci. Un utilisateur mal intentionné peut, par le biais d'une signature judicieusement composée, réaliser un débordement de mémoire lors de l'ouverture de ce message d'avertissement entraînant ainsi l'exécution de code arbitraire avec les privilèges de l'utilisateur ayant reçu ce courrier.

## **5 Solution**

Appliquer le correctif distribué par Microsoft (cf. section Documentation).

## **6 Documentation**

Bulletin de sécurité Microsoft :

<http://www.microsoft.com/technet/security/bulletin/ms02-058.asp>

## **Gestion détaillée du document**

**11 octobre 2002** version initiale.