



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 juillet 2000
N° CERTA-2000-AVI-015

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans l'en-tête des mès sous 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-2000-AVI-015>

Gestion du document

Référence	CERTA-2000-AVI-015
Titre	Vulnérabilité dans l'en-tête des mès sous Outlook
Date de la première version	19 juillet 2000
Date de la dernière version	–
Source(s)	Microsoft Security Bulletin
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 en chargeant son courrier depuis sa boîte aux lettres.

2 Systèmes affectés

- Microsoft Outlook 97, 98, 2000
- Microsoft Outlook Express 4.0, 4.01, 5.0, 5.01

3 Résumé

Une vulnérabilité a été découverte sous Outlook et Outlook Express permettant à un utilisateur malveillant d'exécuter du code sur une machine distante. Le code peut s'exécuter même si on ne lit par le message et les pièces jointes.

4 Description

Un composant partagé par Outlook et Outlook Express utilise une mémoire tampon, dont le débordement n'est pas contrôlé, qui contient les en-têtes des mès téléchargés en POP3 ou IMAP4. En provoquant un débordement de cette mémoire tampon, un utilisateur mailvaillant, expédiant un mël, peut stopper l'application ou exécuter du code sur la machine destinataire.

Cette vulnérabilité fonctionne même si le mël n'est pas lu, le code malicieux se trouvant dans l'en-tête. En particulier ce problème n'est pas lié aux recommandations de la note CERTA-2000-INF-002 concernant les pièces jointes.

Nota : Les utilisateurs d'Internet Explorer 5.01 Service Pack 1 ou les utilisateurs Internet Explorer 5.5 (sauf sous Windows 2000) ne sont pas affectés par cette vulnérabilité.

5 Solution

Cette vulnérabilité peut être éliminée par l'installation par défaut de :

- Internet Explorer 5.01 Service Pack 1

<http://www.microsoft.com/Windows/ie/download/ie501sp1.htm>

- Internet Explorer 5.5 sur tous systèmes (excepté Windows 2000*)

<http://www.microsoft.com/Windows/ie/download/ie55.htm>

* Lors de l'installation d'Internet Explorer 5.5 sous Windows 2000 la version corrigée d'Outlook Express n'est pas installée. La vulnérabilité est donc toujours présente. Windows 2000 Service Pack 1, qui n'est pas encore disponible en France, prendra cette correction en compte.

6 Documentation

- Bulletin Microsoft

<http://www.microsoft.com/technet/security/bulletin/MS00-043.asp>

Gestion détaillée du document

19 juillet 2000 version initiale.