Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 octobre 2005
N° CERTA-2005-AVI-399

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité d'un composant Microsoft Windows et Exchange Server

Gestion du document

Référence	CERTA-2005-AVI-399
Titre	Vulnérabilité d'un composant Microsoft Windows et Exchange Server
Date de la première version	12 octobre 2005
Date de la dernière version	–
Source(s)	Avis MS05-048 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,
- déni de service.

2 Systèmes affectés

- Microsoft Windows 2000,
- Microsoft Windows XP toutes architectures,
- Microsoft Windows 2003 toutes architecture,
- Microsoft Exchange 2000 Server SP3 avec le correctif global (« Post-SP3 Update Rollup ») d'août 2004.

3 Résumé

Une vulnérabilité d'un composant COM (« Component Object Model ») permet l'exécution de code arbitraire à l'aide d'un message SMTP (protocole de messagerie internet le plus courant) malicieusement construit.

4 Description

Le composant en question est CDO (« Collaboration Data Objects ») et offre une bibliothèque pour la création et la modification de messages internet. Une mauvaise gestion d'un tampon mémoire permet à un utilisateur mal intentionné d'exécuter du code et d'obtenir alors un contrôle total du système.

5 Contournement provisoire

Désactiver les récepteurs des événements de transport (« event sinks ») en se référant à la procédure décrite dans le bulletin de sécurité de l'éditeur (cf. section Documentation).

6 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

7 Documentation

- Bulletin de sécurité Microsoft MS05-048 du 11 octobre 2005 :
  http://www.microsoft.com/technet/security/Bulletin/MS05-048.mspx
- Article en français de la base de connaissance sur l'énumération des récepteurs d'événements de transport enregistrés :
  http://support.microsoft.com/default.aspx?scid=kb;fr;f258224
- Référence CVE CAN-2005-1987 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1987

Gestion détaillée du document

12 octobre 2005 version initiale.