

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans Microsoft Exchange

---

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-2009-AVI-060>

---

### Gestion du document

Référence	CERTA-2009-AVI-060
Titre	Multiples vulnérabilités dans Microsoft Exchange
Date de la première version	11 février 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS09-003 du 10 février 2009
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 à distance.

## 2 Systèmes affectés

- Microsoft Exchange 2000 Server Service Pack 3 ;
- Microsoft Exchange 2003 Server Service Pack 2 ;
- Microsoft Exchange 2007 Server Service Pack 1 versions 32-bit et x64.

## 3 Résumé

Deux vulnérabilités présentes dans Microsoft Exchange Server permettent à un utilisateur distant de provoquer un déni de service ou d'exécuter du code arbitraire.

## 4 Description

Deux vulnérabilités sont présentes dans Microsoft Exchange Server :

- la première est relative à une faiblesse dans l'interpréteur de commande MAPI (Messaging Application Programming Interface) et permet à un utilisateur distant de provoquer un déni de service des composants de Microsoft Exchange s'appuyant sur EMSMDB32 comme Attendant Service;
- la seconde concerne la mise en œuvre du protocole TNEF (Transport Neutral Encapsulation Format) et permet à un utilisateur distant d'exécuter du code arbitraire à distance avec les privilèges du service Exchange par le biais d'un message TNEF construit de façon particulière.

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité Microsoft MS09-003 du 10 février 2009 :  
<http://www.microsoft.com/france/technet/security/Bulletin/MS09-003.msp>  
<http://www.microsoft.com/technet/security/Bulletin/MS09-003.msp>
- Référence CVE CVE-2009-0098 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0098>
- Référence CVE CVE-2009-0099 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0099>

## Gestion détaillée du document

11 février 2009 version initiale.