



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 24 octobre 2005  
N° CERTA-2005-AVI-403-001

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans Microsoft Windows MSDTC et COM+

---

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-403>

---

### Gestion du document

Référence	CERTA-2005-AVI-403-001
Titre	Multiples vulnérabilités dans Microsoft Windows MSDTC et COM+
Date de la première version	12 octobre 2005
Date de la dernière version	24 octobre 2005
Source(s)	Bulletin de sécurité Microsoft MS05-051
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

- Elevation de privilèges ;
- déni de service ;
- exécution de commandes arbitraire locale ou distante ;
- accès illégal au système.

## 2 Systèmes affectés

- Microsoft Windows XP Professional ;
- Microsoft Windows XP Home Edition ;
- Microsoft Windows Server 2003 Web Edition ;
- Microsoft Windows Server 2003 Standard Edition ;
- Microsoft Windows Server 2003 Enterprise Edition ;
- Microsoft Windows Server 2003 Datacenter Edition ;
- Microsoft Windows Server 2000 Server ;
- Microsoft Windows Server 2000 Professional ;
- Microsoft Windows Server 2000 Advanced Server ;
- Microsoft Windows Server 2000 Datacenter Server.

### 3 Résumé

Les services MSDTC et COM+ sont vulnérables à de multiples vulnérabilités, pouvant être exploitées en local ou à distance par un utilisateur malveillant.

### 4 Description

- Une mauvaise gestion de la pile dans MSDTC (*Microsoft Distributed Transaction Coordinator*) peut être exploitée par un utilisateur mal intentionné afin d'exécuter du code arbitraire en local et/ou élever ses privilèges. Cette vulnérabilité touche les versions suivantes de Microsoft :
  - Windows 2000 ;
  - Windows XP Service Pack 1 ;
  - Windows Server 2003.
- Une erreur dans le composant COM+ peut être exploitée par un utilisateur mal intentionné afin d'exécuter du code arbitraire à distance par le biais d'un paquet réseau spécialement conçu, ou en local par le biais d'une application spécialement construite. Cette vulnérabilité touche les versions suivantes de Microsoft :
  - Windows 2000 (exécution de code à distance) ;
  - Windows XP Service Pack 1 (exécution de code à distance);
  - Windows XP Service Pack 2 (exécution de code en local);
  - Windows Server 2003 (exécution de code en local);
  - Windows Server 2003 Service Pack 1 (exécution de code en local).
- Une erreur dans la validation des requêtes TIP (*Transaction Internet Protocol*) par MSDTC peut être exploitée à distance, via un paquet malicieusement construit, afin de bloquer les réponses du service. Le paquet malicieux peut être transféré aux autres machines du réseau à travers la première machine affectée, ce qui aura pour cause l'arrêt de MSDTC sur l'ensemble de ces machines.  
Les machines n'interprétant pas le protocole TIP ne sont pas vulnérables.

### 5 Solution

Appliquer les correctifs comme indiqué par l'éditeur (cf. Documentation).

### 6 Documentation

- Bulletin de sécurité Microsoft numéro MS05-051 :  
<http://www.microsoft.com/technet/security/Bulletin/MS05-051.msp>
- Bulletin de sécurité Microsoft KB #909444 :  
<http://www.microsoft.com/technet/security/advisory/909444.msp>
- Détails sur le bulletin de sécurité Microsoft #909444 :  
<http://support.microsoft.com/kb/909444>

### Gestion détaillée du document

**12 octobre 2005** version initiale.

**24 octobre 2005** ajout du bulletin de sécurité #909444 Microsoft.