



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 mai 2006
N° CERTA-2006-AVI-189

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités du service Windows MSDTC

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-2006-AVI-189>

Gestion du document

Référence	CERTA-2006-AVI-189
Titre	Multiples vulnérabilités du service Windows MSDTC
Date de la première version	10 mai 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS06-018 du 09 Mai 2006
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 Windows 2000 Service Pack 4 ;
- Microsoft Windows XP Service Pack 1 ;
- Microsoft Windows XP Service Pack 2 ;
- Microsoft Windows Server 2003 ;
- Microsoft Windows Server 2003 (Itanium).

3 Résumé

Deux vulnérabilités ont été identifiées dans le service MSDTC de Microsoft Windows. Ces deux vulnérabilités peuvent être utilisées par un utilisateur mal intentionné afin de provoquer un déni de service et/ou exécuter du code arbitraire à distance.

4 Description

Deux vulnérabilités ont été identifiées dans Microsoft Windows MSDTC (Microsoft Distributed Transaction Coordinator):

- La première consiste en une erreur présente au niveau de la fonction `CRpcIoManagerServer::BuildContext`
- La deuxième consiste en une erreur présente au niveau de la fonction `MIDL_user_allocate`

Ces deux erreurs sont issues d'une mauvaise gestion de certains messages malformés. Ces deux vulnérabilités peuvent être utilisées par un utilisateur mal intentionné afin de provoquer un déni de service et/ou exécuter du code arbitraire à distance.

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 MS06-018 du 10 mai 2006 :
<http://www.microsoft.com/france/technet/securite/MS06-018.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS06-018.msp>
- Référence CVE CVE-2006-0034 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0034>
- Référence CVE CVE-2006-1184 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1184>

Gestion détaillée du document

10 mai 2006 version initiale.