

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du service Station de Travail de Microsoft Windows

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-499>

Gestion du document

Référence	CERTA-2006-AVI-499
Titre	Vulnérabilité du service Station de Travail de Microsoft Windows
Date de la première version	15 novembre 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS06-070 du 14 novembre 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.

2 Systèmes affectés

- Microsoft Windows 2000 Service Pack 4 ;
- Microsoft Windows XP Service Pack 2.

3 Résumé

Une vulnérabilité a été identifiée dans le service Station de Travail (ou *Workstation Service*) de Microsoft Windows. Une personne malveillante, qui exploiterait celle-ci, pourrait, sous certaines conditions, exécuter des commandes arbitraires à distance sur le système vulnérable.

4 Description

Une vulnérabilité a été identifiée dans le service Station de Travail (ou *Workstation Service*) de Microsoft Windows. Ce service permet de créer et maintenir des connexions des clients Windows vers des serveurs distants.

Un tampon ne serait pas correctement vérifié. L'exploitation de cette vulnérabilité pourrait provoquer un débordement de mémoire, et permettrait, à une personne maveillante distante, de prendre le contrôle complet du système vulnérable.

5 Solution

Se référer au bulletin de sécurité MS06-070 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS06-070 du 14 novembre 2006 :
<http://www.microsoft.com/france/technet/security/bulletin/MS06-070.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS06-070.msp>
- Référence CVE CVE-2006-4691 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4691>

Gestion détaillée du document

15 novembre 2006 version initiale.