Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 23 août 2002
N° CERTA-2002-AVI-186

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le contrôle ActiveX TSAC

Gestion du document

Référence	CERTA-2002-AVI-186
Titre	Vulnérabilité dans le contrôle ActiveX TSAC
Date de la première version	23 août 2002
Date de la dernière version	–
Source(s)	Avis Microsoft MS02-046
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.

2 Systèmes affectés

Tous les systèmes Windows.

3 Résumé

Une vulnérabilité dans le contrôle ActiveX `Terminal Services Advanced Client` (TSAC) permet à un utilisateur mal intentionné d'exécuter du code arbitraire sur le système.

4 Description

Le contrôle web du `Terminal Services Advanced Client` (TSAC) est un contrôle ActiveX qui peut être utilisé pour lancer des sessions `Terminal Services` dans `Internet Explorer`. Le contrôle TSAC n'est pas installé par défaut sur les systèmes Windows client. Dès lors qu'un client Windows se connecte à un

serveur IIS qui utilise le contrôle TSAC, le téléchargement depuis le serveur et l'installation du contrôle TSAC sont réalisés par le client.

Le contrôle TSAC contient une vulnérabilité de type débordement de mémoire. Cette vulnérabilité permet à un utilisateur mal intentionné d'exécuter du code arbitraire sur le système client dans le contexte de sécurité de l'utilisateur connecté.

5 Solution

Télécharger le correctif.

- Pour les webmestres qui utilisent TSAC sur leur site :
  http://www.microsoft.com/windowsxp/pro/downloads/rdwebconn.asp
- Pour les utilisateurs d'Internet Explorer :
  http://www.microsoft.com/windows/ie/downloads/critical/q323759ie/default.asp

6 Documentation

Avis de sécurité Microsoft MS02-046 :
http://www.microsoft.com/technet/security/bulletin/MS02-046.asp

Gestion détaillée du document

23 août 2002 version initiale.