Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 09 novembre 2000
N° CERTA-2000-AVI-070

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité sous Microsoft Windows NT4.0 Terminal Server

Gestion du document

Référence	CERTA-2000-AVI-070
Titre	Vulnérabilité sous Microsoft Windows NT4.0 Terminal Server
Date de la première version	09 novembre 2000
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft
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 ;
- Compromission des données.

2 Systèmes affectés

Microsoft Windows NT 4.0 Terminal Server

3 Résumé

NT 4.0 Terminal Server est un serveur de terminal permettant à un poste client distant de disposer d'une machine virtuelle NT.

Un utilisateur mal intentionné peut provoquer à distance un débordement de pile sur un système Windows NT 4.0 Terminal Server, afin d'exécuter du code arbitraire.

4 Description

Sous Windows NT 4.0 Terminal Server, la procédure de connexion ne vérifie pas correctement certaines variables d'environnement transmises par le client. Un utilisateur mal intentionné peut fabriquer une requête provoquant un débordement de pile et exécuter du code arbitraire sur la machine cible.

Cette vulnérabilité permet d'ajouter, de modifier ou de changer les données sur le disque de la machine cible ainsi que la prise de contrôle du système avec les privilèges administrateur.

Nota : Il n'est pas nécessaire de réussir une authentification pour mettre en oeuvre cette vulnérabilité.

5 Contournement provisoire

Par défaut NT 4.0 Terminal Server ouvre le port tcp 3389.
Filtrer ce port au niveau du garde barrière, afin d'éviter une attaque provenant d'internet.

6 Solution

Correctif :
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=25565

7 Documentation

Bulletin de sécurité Microsoft :
http://www.microsoft.com/technet/security/bulletin/MS00-087.ASP

Gestion détaillée du document

09 novembre 2000 version initiale.