Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 septembre 2000
N° CERTA-2000-AVI-048

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du client telnet sous Windows 2000

Gestion du document

Référence	CERTA-2000-AVI-048
Titre	Vulnérabilité du client telnet sous Windows 2000
Date de la première version	15 septembre 2000
Date de la dernière version	–
Source(s)	Bugtraq 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

Usurpation d'identité, et vol de mot de passe.

2 Systèmes affectés

Windows 2000.

3 Résumé

Une vulnérabilité du client telnet sous Windows 2000 a été décelée. Elle réside dans le fait qu'il effectue par défaut, et sans intervention de l'utilisateur, une authentification NTLM (*NT Lan Manager*) lorsqu'il se connecte à un serveur telnet sous windows 2000.

4 Description

Un utilisateur mal intentionné peut, en simulant un serveur telnet sous windows 2000, faire émettre à tout poste possédant un client telnet (installé par défaut), une réponse d'authentification NTLM pour une ouverture de session, à l'insu de la victime.

L'utilisateur malicieux pourrait alors déchiffrer le mot de passe.

Une autre attaque consiste à soumettre au client telnet sous windows 2000 le challenge envoyé à l'utilisateur malicieux par un serveur sur lequel la victime possède un compte, afin d'utiliser la réponse d'authentification pour ouvrir une session sous l'identité de la victime.

La demande d'ouverture de session peut être très simplement camouflée dans un lien sur une page web (voire dans un contrôle Active X) lue par la victime à travers son navigateur ou son client de messagerie.

5 Contournement provisoire

Supprimer le client telnet s'il n'est jamais utilisé sur le poste sous windows 2000.

6 Solution

Appliquer le correctif Microsoft :
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=24319

7 Documentation

Bulletin de sécurité Microsoft et sa FAQ :

- http://www.microsoft.com/technet/security/bulletin/ms00-067.asp
- http://www.microsoft.com/technet/security/bulletin/fq00-067.asp

Gestion détaillée du document

15 septembre 2000 version initiale.