Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 08 juin 2001
N° CERTA-2001-AVI-060

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de telnet sous Windows 2000

Gestion du document

Référence	CERTA-2001-AVI-060
Titre	Multiples vulnérabilités du service telnet sous Windows 2000
Date de la première version	08 juin 2001
Date de la dernière version	–
Source(s)	Bulletin de Sécurité Microsoft MS01-031
Pièce(s) jointe(s)	Aucune

TAB. 1 – *gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risques

- Déni de service ;
- divulgation d'informations ;
- élévation de privilèges.

2 Systèmes affectés

Toutes les versions de Windows 2000.

3 Résumé

Deux vulnérabilités du service `telnet` sous Windows 2000 permettent à un utilisateur mal intentionné d'élever ses privilèges.

Quatre autres vulnérabilités permettent d'effectuer un déni de service.

Enfin la dernière vulnérabilité permet à un utilisateur mal intentionné d'obtenir d'un serveur des informations auxquelles il n'a normalement pas le droit d'accéder.

4 Description

– Les deux premières vulnérabilités proviennent d'un problème dans la gestion des sessions `telnet`.
L'ouverture d'une session `telnet` crée un « tube nommé » (*FIFO*) dont le nom est prévisible et utilisable par n'importe quel programme qui lui est associé.
Le service `telnet` fonctionne avec les privilèges de `Local System` et utilise ce tube sans plus de vérifications dans ce contexte de sécurité.
Un utilisateur mal intentionné ayant le droit d'exécuter du code sur le serveur peut développer un programme qui crée un tel tube nommé afin que le service `telnet` l'utilise lors de la prochaine session `telnet`, ou bien un programme auquel il associe le tube nommé qui sera créé lors de la prochaine ouverture de session `telnet`.
Dans les deux cas, l'utilisateur mal intentionné exécute son programme dans le contexte de sécurité de `Local System`.

– Les quatre suivantes permettent d'empêcher le service `telnet` de fonctionner correctement.

  – Un utilisateur mal intentionné peut, en créant un nombre suffisant de sessions inactives, empêcher le service d'arrêter ce type de session quelqu'en soit le propriétaire.
  – Il est aussi possible, en démarrant puis arrêtant successivement et rapidement suffisamment de sessions, d'empêcher le service de traiter les sessions effectives.
  – Un utilisateur mal intentionné peut aussi créer une « violation d'accès » en envoyant une commande de *logon* habilement construite.
  – Enfin, un appel système ayant pour effet d'arrêter une session `telnet` peut être effectué avec les privilèges d'un utilisateur normal.

– Un utilisateur mal intentionné peut facilement détecter la présence d'un compte `invité` s'il est activé, en se connectant au serveur Windows 2000 comme un utilisateur de domaine au lieu de s'identifier comme un utilisateur local.

5 Contournement provisoire

– Afin d'éviter une élévation de privilèges via la vulnérabilité du « tube nommé », ainsi que le déni de service par l'appel système particulier, il faut interdire tout utilisateur d'exécuter du code sur tous les serveur.
– Désactiver le compte `invité` dont le mot de passe par défaut est facile à connaître.

6 Solution

Appliquer le correctif de Microsoft :
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=30508

7 Documentation

Bulletin de sécurité Microsoft :
http://www.microsoft.com/technet/security/bulletin/ms01-031.asp

Gestion détaillée du document

08 juin 2001 version initiale.