Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 26 mars 2001
N° CERTA-2001-ALE-002

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Risque d'exploitation des ressources partagées sous Windows

Gestion du document

Référence	CERTA-2001-ALE-002
Titre	Risque d'exploitation des ressources partagées sous Windows
Date de la première version	26 mars 2001
Date de la dernière version	–
Source(s)	
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

- Publication de la liste des ressources partagées de vos réseaux ;
- accès en lecture ou en écriture à vos ressources.

2 Systèmes affectés

Touts les systèmes Windows.

3 Résumé

Un utilitaire téléchargeable sur un site commercial *scanne* les ressources partagées des machines connectées à Internet et les publie dans un groupe de discussion (*newsgroups*).

4 Description

Netbios est un protocole utilisé essentiellement sur les systèmes Windows. Il permet de partager des ressources (répertoires, imprimantes, etc.). La compatibilité est offerte à d'autres systèmes grâce à des outils comme SAMBA.

NetBios est conçu à l'origine pour s'appuyer sur la couche réseau NetBEUI qui n'est pas routable. Windows permet d'offrir le protocole NetBios sur la couche IP ou IPX. Dès lors, une ressource NetBios sur une machine connectée à Internet est visible du monde entier.

Quelques outils permettent de balayer (*scanner*) des adresses IP pour découvrir quelles sont les ressources NetBios offertes. Ces outils sont déjà dangereux.

Dans le cas du logiciel `ShareSniffer`, les résultats de ces *scans* sont postés automatiquement sur un forum à la fin de chaque session. Les ressources partagées ainsi détectées sont connues par un grand public, et peuvent alors être exploitées facilement.

Le danger lié à la publication de vos ressources est déjà grand. Mais la société ShareSniffer va plus loin en propageant l'idée qu'utiliser les ressources partagées d'ordinateurs mal configurés est légitime.

Il est probable que de nombreux naïfs ou faux naïfs vont se laisser abuser par ce type de discours.

En particulier un répertoire partagé sur vos machines pourrait être exploité pour faire un serveur de fichiers (MP3 par exemple). Les risques inhérents sont une augmentation phénoménale des coûts de connexion et une diminution sensible de la bande passante de votre réseau dues au trafic engendré par cette exploitation de vos ressources (et d'attirer les foudres des ayants droits) et un accroissement sensible du trafic montant.

5 Solution

- Bloquer les ports concernant Netbios sur le garde-barrière : 135, 137, 138, 139 TCP et UDP.
- Mettre à niveau les règles de sécurité sur les fichiers et principalement les ressources partagées :
  - Supprimer les partages non authentifiés ;
  - mettre des mots de passe sur tout partage Windows 9x ;
  - renforcer les mots de passe existants ;
  - resserrer les permissions sur les partages de Windows NT/2000.

Gestion détaillée du document

26sx mars 2001 version initiale.