Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 novembre 2000
N° CERTA-2000-AVI-074

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité sous Windows 2000 dans l'authentification NTLM

Gestion du document

Référence	CERTA-2000-AVI-074
Titre	Vulnérabilité sous Windows 2000 dans l'authentification NTLM
Date de la première version	22 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

Contournement des règles de sécurité

2 Systèmes affectés

- Windows 2000 Professionnal, Service pack 1 ;
- Windows 2000 Server, Service pack 1 ;
- Windows 2000 Advanced Server, Service pack 1 ;
- Windows 2000 Datacenter, Service pack 1.

3 Résumé

Un utilisateur mal intentionné peut par une attaque de force brute trouver le login (utilisateur - mot de passe) d'une machine sous Windows 2000, membre d'un domaine mixte (Windows 2000 - WIndows NT).

4 Description

L'authentification utilisé par Windows 2000 est Kerberos, cependant afin de garantir une compatibilité entre les clients, serveurs, et contrôleurs de domaine Windows 2000 ainsi que les systèmes fonctionnant avec Windows NT, l'authentification NTLM (NT Lan Manager) est supportée.

Un utilisateur mal intentionné peut contourner les règles de sécurité (verrouillage des comptes après plusieurs tentatives) et attaquer par force brute les comptes utilisateurs afin de découvrir l'identifiant et son mot de passe.

Cette vulnérabilité affecte uniquement les systèmes Windows 2000 membres d'un domaine mixte.
Windows 2000 Gold n'est pas affecté.

5 Solution

Correctif fourni par Microsoft :
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=25606

6 Documentation

Le bulletin de sécurité Microsoft :
http://www.microsoft.com/technet/security/bulletin/ms00-089.asp
La FAQ :
http://www.microsoft.com/technet/security/bulletin/fq00-089.asp

Gestion détaillée du document

22 novembre 2000 version initiale.