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 février 2001
N° CERTA-2001-AVI-015

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Windows NT 4 dans l'authentification NTLM

Gestion du document

Référence	CERTA-2001-AVI-015
Titre	Vulnérabilité de Windows NT 4 dans l'authentification NTLM
Date de la première version	08 février 2001
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS01-008
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

2 Systèmes affectés

- Windows NT 4.0 Workstation ;
- Windows NT 4.0 Server ;
- Windows NT 4.0 Server Entreprise Edition ;
- Windows NT 4.0 Terminal Server Edition.

3 Résumé

Un utilisateur mal intentionné peut, par le biais d'une vulnérabilité dans l'authentification NTLM, exécuter du code arbitraire avec des privilèges élevés sur la machine cible.

4 Description

Une vulnérabilité de l'authentification NTLM (NT Lan Manager) permet à un utilisateur, disposant d'un compte sur la machine cible, d'exécuter du code arbitraire avec les privilèges «local system».

L'utilisation d'un programme spécifique permet d'émettre des requêtes au NTLM Security Support Provider afin d'exécuter le code de son choix. Il est impératif que l'attaquant dispose d'un compte valide sur la machine cible pour réussir cet exploit.

5 Contournement provisoire

En règle générale, il ne faut pas laisser des utilisateurs sans privilège accéder localement à un serveur ou les autoriser à y exécuter du code à distance (rcmd, NDDE, etc.). Si cette règle est appliquée, elle limitera nettement les dégâts possibles de ce type de vulnérabilités.

6 Solution

Télécharger le correctif sur le site Microsoft (version US) :
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=27804

Nota : Le correctif pour Windows NT 4.0 Terminal Server n'est pas encore disponible sur le site.

7 Documentation

Bulletin de sécurité Microsoft :
http://www.microsoft.com/technet/security/bulletin/ms01-008.asp

Faq Microsoft :
http://www.microsoft.com/technet/security/bulletin/fq01-008.asp

Gestion détaillée du document

08 février 2001 version initiale.