Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 janvier 2001
N° CERTA-2001-AVI-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de l'authentification NTLM sous Windows

Gestion du document

Référence	CERTA-2001-AVI-002
Titre	Vulnérabilité de l'authentification NTLM sous Windows
Date de la première version	12 janvier 2001
Date de la dernière version	–
Source(s)	Bulletin Microsoft MS01-001
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 mécanismes d'authentification.

2 Systèmes affectés

- Office 2000 ;
- Windows 2000 ;
- Windows Millenium Edition.

3 Résumé

Un concepteur d'un site web peut, par le biais d'une vulnérabilité dans l'authentification NTLM, obtenir les informations d'authentification d'un utilisateur navigeant sur le site.

4 Description

Un composant (Web Extender Client) est installé lors de la mise en place d'Office 2000, Windows 2000 et Windows M.E. Ce composant apporte des facilités sous Internet Explorer comme la présentation, la copie ou la

modification des fichiers via HTTP avec une présentation identique à l'explorateur Windows.

La gestion de l'authentification NTLM (NT Lan Manager) sous WEC présente une vulnérabilité en ne tenant pas compte de la configuration d'Internet Explorer concernant l'authentification NTLM.

Un concepteur de site mal intentionné peut donc faire effectuer systématiquement l'authentification et récupérer les paramètres d'authentification dans le but de les transformer en identification en clair.

5 Contournement provisoire

Bloquer le trafic NetBIOS au niveau du garde barrière.

6 Solution

Correctif pour Office 2000 (version internationale) :
http://officeupdate.microsoft.com/2000/downloaddetail/wecsec.htm

Correctif pour Windows 2000 (version US) (sans office 2000) :
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=26889

Correctif pour Windows M.E (version US) (sans office 2000) :
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=26705

7 Documentation

Bulletin de sécurité Microsoft :
http://www.microsoft.com/technet/security/bulletin/ms01-001.asp

FAQ Microsoft :
http://www.microsoft.com/technet/security/bulletin/fq01-001.asp

Gestion détaillée du document

12 janvier 2001 version initiale.