Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 avril 2001
N° CERTA-2001-AVI-046

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans WebDAV Service Provider

Gestion du document

Référence	CERTA-2001-AVI-046
Titre	Vulnérabilité dans WebDAV Service Provider
Date de la première version	20 avril 2001
Date de la dernière version	–
Source(s)	Bulletin Microsoft MS01-022
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

Accès aux données.

2 Systèmes affectés

- Microsoft Windows 9x ;
- Microsoft Windows NT ;
- Microsoft Windows Me ;
- Microsoft Windows 2000.

3 Résumé

Un utilisateur mal intentionné peut, par le biais d'un script habilement construit, avoir accès à un réseau WebDav interne avec les privilèges de la machine cible.

4 Description

WebDAV est un standard d'Internet qui permet à plusieurs utilisateurs de coopérer sur des documents en utilisant le système de partage de fichiers.

Théoriquement, WebDAV devrait être capable de faire la différence entre une requête faite par un utilisateur, et une requête faite par un script du navigateur de l'utilisateur.

Néanmoins, du fait d'une faille dans son implémentation, WebDAV traite toutes les requêtes comme étant celles de l'utilisateur.

Il en résulte que si un utilisateur navigue sur une page web ou ouvre un mél écrit en HTML contenant un script, ce script aura accès aux ressources web avec les droits de l'utilisateur.

5 Contournement provisoire

Désactiver l'activation automatique de script dans le navigateur et le logiciel de messagerie.

6 Solution

Correctif Microsoft :
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=29129

7 Documentation

Bulletin Microsoft :
http://www.microsoft.com/technet/security/bulletin/MS01-022.asp

Gestion détaillée du document

20 avril 2001 version initiale.