Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 juillet 2001
N° CERTA-2001-AVI-078

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de l'identification SMTP sous Windows 2000

Gestion du document

Référence	CERTA-2001-AVI-078
Titre	Vulnérabilité de l'identification SMTP sous Windows 2000
Date de la première version	19 juillet 2001
Date de la dernière version	–
Source(s)	Bulletin Microsoft MS01-037
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

- Usurpation d'identité ;
- Risque de diffusion de courrier non sollicité.

2 Systèmes affectés

Microsoft Windows 2000.

3 Résumé

Une vulnérabilité présente dans le protocole d'identification SMTP sous Windows 2000 permet à un utilisateur mal intentionné de s'identifier auprès du serveur de courrier comme un utilisateur connu.

4 Description

SMTP est le protocole utilisé par les serveurs de courrier. Lorsque le service SMTP est installé sous Windows 2000, le serveur virtuel SMTP par défaut est activé.

Sous Windows 2000, il est possible d'utiliser des options de sécurité au niveau d'un serveur virtuel SMTP. Un de ces paramètres permet de spécifier le type d'authentification utilisé pour les messages entrant.

Un utilisateur mal intentionné peut, lors de l'authentification au serveur virtuel SMTP, contourner les mécanismes de vérification et s'enregistrer comme un utilisateur connu. Il a alors la possibilité d'expédier et de recevoir des méls en utilisant le nom de domaine de la machine cible.

Cette vulnérabilité peut être utilisée notamment pour diffuser du courrier non sollicité tout en usurpant le point d'origine du courrier.

Nota :

- Cette vulnérabilité n'affecte pas Microsoft Exchange.
- Les serveurs appartenant à un domaine Windows ne sont pas impactés par cette vulnérabilité.

5 Contournement provisoire

Si ce service n'est pas nécessaire sur une machine Windows 2000, il convient de le stopper.

- Dans le menu `Démarrer`, pointer sur `Programmes`, puis sur `Outils d'administration` et cliquer ensuite sur `Services de composants` ;
- Dans l'arborescence de la console, selectionner `Services (locaux)` ;
- Dans le volet de détails, cliquer avec le bouton droit sur `Simple Mail Transfert Protocol`, puis cliquer sur `Arrêter`.

6 Solution

Télécharger le correctif sur le site Microsoft :
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=31181

7 Documentation

Bulletin Microsoft :
http://www.microsoft.com/technet/security/bulletin/MS01-037.asp

Gestion détaillée du document

19 juillet 2001 version initiale.