Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 février 2002
N° CERTA-2002-AVI-046-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de SMTP pour Microsoft Windows

Gestion du document

Référence	CERTA-2002-AVI-046-001
Titre	Multiples vulnérabilités de SMTP pour Microsoft Windows
Date de la première version	28 février 2002
Date de la dernière version	28 février 2002
Source(s)	Bulletin de sécurité Microsoft MS02-011 Bulletin de sécurité Microsoft MS02-012
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

- Utilisation non autorisée du service (relayage de SPAM...) ;
- déni de service.

2 Systèmes affectés

- Pour l'utilisation non autorisée du service : Windows 2000 et Microsoft Exchange 5.5.
- Pour le déni de service : Windows 2000, Windows XP Pro et Microsoft Exchange 2000.

3 Résumé

- Sur les systèmes Windows 2000 et les serveurs Exchange 5.5, il est possible d'utiliser le service SMTP sans autorisation.
- Sur les systèmes Windows 2000, XP Pro et les serveurs Exchange 2000, il est possible d'arrêter à distance et sans authentification le service SMTP (installé par défaut sur ces systèmes).

4 Description

Le service SMTP est le service de messagerie (envoi et relayage de courrier électronique). Il est installé par défaut sur tous les systèmes Windows 2000 Server. Il peut avoir été installé à la demande sur les systèmes Windows XP Pro et Windows 2000 Professional Edition.

- Une vulnérabilité du système d'authentification par NTLM du service SMTP sur le système Windows 2000 et sur le serveur Exchange 5.5 permet à un utilisateur mal intentionné non authentifié d'obtenir les privilèges d'un utilisateur de ce service. Il peut ainsi, par exemple, l'utiliser comme relais de messagerie.
- Sur les systèmes Windows 2000, XP Pro et sur le serveur Exchange 2000, un utilisateur mal intentionné peut, au moyen d'une commande SMTP habilement transformée, arrêter le service SMTP à distance et sans authentification.

5 Contournement provisoire

Arrêter le service SMTP s'il n'est pas utilisé sur les systèmes Windows 2000 et XP Pro du réseau.

6 Solution

Appliquer le correctif de Microsoft selon le système affecté :

- Pour Windows 2000 Server, Advanced Server et Professional Edition (avec ou sans Microsoft Exchange 2000) :
  http://www.microsoft.com/Downloads/Release.asp?ReleaseID=36556
  Le serveur Exchange 2000 ne peut être installé que sur Windows 2000, et utilise le service SMTP natif de celui-ci. Appliquer le correctif au système Windows 2000 revient à supprimer la vulnérabilité du serveur Exchange 2000.
- Pour Exchange Server 5.5 (indépendamment du système sur lequel il est installé) :
  http://www.microsoft.com/Downloads/Release.asp?ReleaseID=33423
  Le service SMTP de Exchange 5.5 est indépendant de celui présent sous Windows 2000. Pour supprimer la vulnérabilité de Exchange 5.5 installé sur un système Windows 2000, il n'est pas nécessaire d'appliquer le correctif pour Windows 2000.
- Pour Windows XP Pro :
  http://www.microsoft.com/Downloads/Release.asp?ReleaseID=36636

7 Documentation

- Le bulletin de sécurité Miscrosoft MS02-011 concernant l'utilisation non autorisée du service SMTP :
  http://www.microsoft.com/technet/security/bulletin/MS02-011.asp
- Le bulletin de sécurité Miscrosoft MS02-012 concernant le déni de service possible sur SMTP :
  http://www.microsoft.com/technet/security/bulletin/MS02-012.asp

Gestion détaillée du document

28 février 2002 version initiale.

28 février 2002 seconde version : Ajout d'informations concernant le correctif pour Exchange 2000 et Exchange 5.5 sur Windows 2000.