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 juillet 2006
N° CERTA-2006-AVI-283

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités du service Serveur de Microsoft Windows

Gestion du document

Référence	CERTA-2006-AVI-283
Titre	Multiples vulnérabilités du service Serveur de Microsoft Windows
Date de la première version	12 juillet 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft du 11 juillet 2006
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 à distance.

2 Systèmes affectés

- Microsoft Windows 2000 Service Pack 4 ;
- Microsoft Windows XP Service Pack 1 et Service Pack 2 ;
- Microsoft Windows Server 2003 et Microsoft Windows Server 2003 Service Pack 1 ;
- Microsoft Windows Server 2003 pour les systèmes Itanium ou Édition x64 ;

Les systèmes d'exploitation Microsoft Windows 98, Microsoft Windows 98 Deuxième Édition (SE) et Microsoft Windows Millennium Edition (ME) ne sont pas concernés.

3 Description

Deux vulnérabilités ont été identifiées dans Microsoft Windows. Elles concernent le service Serveur, qui est installé par défaut sur la plupart des systèmes Windows.

– La première vulnérabilité vise les `mailslots`. Un mailslot est un mécanisme temporaire utilisé par les applications et les processus pour faciliter le transfert de données unidirectionnel. Le service ne contrôlerait pas correctement la taille d'un paramètre. Cette vulnérabilité peut être exploitée par une personne malveillante distante, qui, en envoyant un paquet réseau spécialement conçu, pourrait exécuter du code arbitraire sur le système affecté.
– La deuxième vulnérabilité concerne SMB (pour *Server Message Block*). Il s'agit du protocole standard Internet utilisé par Windows pour partager des fichiers, des imprimantes et des ports série et pour la communication entre les ordinateurs. Il fonctionne en mode requête-réponse entre client et serveur. Le service Serveur n'initialiserait pas correctement un espace mémoire. Une personne malveillante pourrait exploiter cette vulnérabilité afin de lire à distance les informations stockées dans les tampons pour le trafic Server Message Block.

4 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

5 Documentation

– Bulletin de sécurité Microsoft MS06-035 du 11 juillet 2006 :
http://www.microsoft.com/france/technet/security/Bulletin/MS06-035.mspx
http://www.microsoft.com/technet/security/Bulletin/MS06-035.mspx
– Référence CVE CVE-2006-1314 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1314
– Référence CVE CVE-2006-1315 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1315

Gestion détaillée du document

12 juillet 2006 version initiale.