



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 septembre 2006
N° CERTA-2006-AVI-338-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le Service Serveur de Microsoft Windows

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2006-AVI-338>

Gestion du document

Référence	CERTA-2006-AVI-338-001
Titre	Vulnérabilité dans le Service Serveur de Microsoft Windows
Date de la première version	09 août 2006
Date de la dernière version	13 septembre 2006
Source(s)	Bulletin de sécurité Microsoft MS06-040 du 08 août 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 XP Professional x64 Edition ;
- Microsoft Windows Server 2003 (Service Pack 1 inclus) ;
- Microsoft Windows Server 2003 x64 Edition et Itanium Edition.

3 Résumé

Une vulnérabilité est identifiée dans le `Server Service` de Microsoft Windows. Une personne malveillante pourrait l'exploiter afin d'exécuter du code arbitraire à distance et prendre le contrôle complet de la machine vulnérable.

4 Description

Une vulnérabilité de type débordement de tampon a été identifiée dans le `Server Service` du système d'exploitation Microsoft Windows. Ce service est utilisé pour les `RPC (Remote Procedure Call)`, et de manière plus générale, pour le partage de ressources (fichiers, imprimantes, etc) dans un réseau local. Il est accessible à distance par les ports `139/tcp` et `445/tcp`.

Une personne malveillante exploitant cette vulnérabilité pourrait exécuter du code arbitraire à distance, voire prendre le contrôle intégral de la machine vulnérable.

Cette vulnérabilité est différente de celle évoquée dans le précédent bulletin Microsoft MS06-035 (CERTA-2006-AVI-283). Il est par ailleurs vivement conseillé de bloquer les ports impliqués à la sortie du réseau ou sur les machines n'utilisant pas ce service.

5 Solution

Se référer au bulletin de sécurité MS06-040 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

Le bulletin de sécurité MS06-040 a été publié de nouveau par Microsoft le 12 septembre 2006. L'application du précédent correctif semblait poser problème avec les versions Microsoft Windows Server 2003 SP1 et Windows XP Professionnel Edition x64. De plus amples informations sont disponibles dans l'article 921883 de la base de données Microsoft.

6 Documentation

- Référence CVE CVE-2006-3439 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3439>
- Bulletin de sécurité Microsoft MS06-040 du 08 août 2006 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS06-040.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS06-040.msp>
- Article 921883 concernant MS06-040 mis à jour le 12 septembre 2006 :
<http://support.microsoft.com/kb/921883>

Gestion détaillée du document

09 août 2006 version initiale.

13 septembre 2006 ajout de la mise à jour du bulletin MS06-040 par Microsoft.