Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 novembre 2006
N° CERTA-2006-AVI-495

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans le service Client pour NetWare de Microsoft Windows

Gestion du document

Référence	CERTA-2006-AVI-495
Titre	Vulnérabilités dans le service Client pour NetWare de Microsoft Windows
Date de la première version	15 novembre 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS06-066 du 14 novembre 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 ;
- déni de service à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- Microsoft Windows 2000 Service Pack 4 ;
- Microsoft Windows XP Service Pack 2 ;
- Microsoft Windows Server 2003 ;
- Microsoft Windows Server 2003 Service Pack 1.

Des versions de Windows qui ne sont plus officiellement maintenues par Microsoft peuvent aussi être affectées.

3 Résumé

Des vulnérabilités ont été identifiées dans le service Client pour NetWare (ou *Client Service for NetWare CSNW*) de Microsoft Windows. Une personne qui exploiterait celles-ci à distance pourrait, sous certaines conditions, exécuter des commandes arbitraires, ou perturber le service.

4 Description

Des vulnérabilités ont été identifiées dans le service Client pour NetWare (ou `CSNW`). CSNW permet un échange d'informations entre des machines Windows et des systèmes Novell NetWare (service d'impression, de stockage, etc). Ce service peut aussi s'appeler *Gateway Service* pour NetWare (GSNW) avec Windows 2000 Server.

Une personne malveillante pourrait construire des paquets particuliers, afin d'exploiter l'une de ces vulnérabilités. Si le système distant est vulnérable, la mauvaise manipulation des données reçues pourrait alors provoquer l'exécution de code arbitraire., ou perturber le service.

5 Solution

Se référer au bulletin de sécurité MS06-066 de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS06-066 du 14 novembre 2006 :
  http://www.microsoft.com/france/technet/security/bulletin/MS06-066.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS06-066.mspx
- Référence CVE CVE-2006-4688 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4688
- Référence CVE CVE-2006-4689 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4689

Gestion détaillée du document

15 novembre 2006 version initiale.