

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Microsoft Network Connection Manager

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-2005-AVI-406>

Gestion du document

Référence	CERTA-2005-AVI-406
Titre	Vulnérabilité de Microsoft Network Connection Manager
Date de la première version	14 octobre 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS05-045
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

- Déni de service par un utilisateur local,
- éventuel déni de service distant par un utilisateur authentifié.

2 Systèmes affectés

- Windows 2000 Service Pack 4,
- Windows XP Service Pack 1 et Service Pack 2,
- Windows 2003 avec ou sans Service Pack 1,
- produits Avaya utilisant Microsoft Windows.

3 Résumé

Le gestionnaire de connexion réseau (« Network Connection Manager ») est vulnérable à une attaque en déni de service lancée en local et éventuellement, selon la version de *Windows*, à distance par un utilisateur authentifié.

4 Description

Le gestionnaire de connexion réseau est un composant du système d'exploitation permettant de contrôler les connexions réseau du système, telles que celles du dossier « Connexions réseau et accès à distance ».

Un bogue dans une bibliothèque peut être utilisé pour bloquer le composant.

Sur les versions vulnérables à distance avec le compte *Invité* activé, ce dernier peut être utilisé par quiconque pour réaliser le déni de service.

5 Contournement provisoire

Filtrer les ports RPC en particulier 135, 137, 138 et 445 en udp et 135, 139, 445 et 593 en tcp voire les ports 80 et 443 tcp sur RPC sur HTTP est présent.

6 Solution

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

7 Documentation

- Bulletin de sécurité Microsoft MS05-045 du 11 octobre 2005 :
<http://www.microsoft.com/technet/security/Bulletin/MS05-045.msp>
<http://www.microsoft.com/france/technet/securite/ms05-045.msp>
- Bulletin de sécurité Avaya ASA-2005-214 du 11 octobre 2005 :
<http://support.avaya.com/elmodocs2/security/ASA-2005-214.pdf>
- Référence CVE CAN-2005-2307 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2307>

Gestion détaillée du document

14 octobre 2005 version initiale.