Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 septembre 2002
N° CERTA-2002-AVI-213

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du protocole RDP dans les systèmes Windows

Gestion du document

Référence	CERTA-2002-AVI-213
Titre	Vulnérabilité du protocole RDP dans les systèmes Windows
Date de la première version	19 septembre 2002
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS02-051
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

– Divulgation d'informations ;
– déni de service.

2 Systèmes affectés

Microsoft Windows 2000 et Windows XP.

3 Résumé

Un utilisateur mal intentionné peut exploiter deux vulnérabilités du protocole RDP pour récupérer des informations ou pour provoquer un déni de service.

4 Description

RDP est un protocole utilisé par les systèmes Windows pour établir des sessions entre un client et un terminal distant.

La première vulnérabilité concerne le chiffrement des sessions RDP. Même si celles-ci sont chiffrées, les empreintes (*checksums*) des données sont envoyées en clair sur le réseau.

Il est alors possible pour un utilisateur mal intentionné, pouvant écouter le réseau, de décrypter l'intégralité de la session.

La deuxième vulnérabilité ne concerne que l'implémentation du protocole RDP sur les systèmes Windows 2000. Elle se situe au niveau du traitement des paquets de données.

Un utilisateur mal intentionné peut envoyer des paquets malicieusement forgés pour provoquer l'arrêt brutal du service *Remote Desktop*, et avec lui, l'arrêt du système.

Cette vulnérabilité peut être exploitée sans authentification préalable.

5 Contournement provisoire

Pour se protéger contre une attaque venant de l'extérieur exploitant la deuxième vulnérabilité, il est recommandé de filtrer le port 3389 (TCP et UDP) sur les pare-feux.

6 Solution

Appliquer le correctif founi par l'éditeur (cf. section Documentation).

7 Documentation

Bulletin de sécurité Microsoft MS02-051 :
http://www.microsoft.com/technet/security/bulletin/MS02-051.asp

Gestion détaillée du document

19 septembre 2002 version initiale.