

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le protocole RDP sous Windows 2000

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-2001-AVI-012>

Gestion du document

Référence	CERTA-2001-AVI-012
Titre	Vulnérabilité dans le protocole RDP sous Windows 2000
Date de la première version	01 février 2001
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft (MS01-006)
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

- Dénis de service ;
- Pertes de données.

2 Systèmes affectés

- Microsoft Windows 2000 Server ;
- Microsoft Windows 2000 Advanced Server.

3 Résumé

Une vulnérabilité dans le protocole RDP sous Windows 2000 permet à un utilisateur mal intentionné de créer un déni de service sur le serveur cible et provoquer une perte des données traitées lors de cette attaque.

4 Description

Le protocole RDP (Remote Desktop Protocol), protocole utilisé par telnet terminal serveur sous Windows ne vérifie pas correctement certaines séries de paquets reçus. Un utilisateur mal intentionné peut, par le biais de

paquets volontairement choisis, entraîner l'arrêt du serveur. Toutes les données des applications tournant sur le serveur à ce moment ne seront pas sauvegardées.

Nota : Il n'est pas nécessaire d'établir une session avec le serveur pour exploiter cette vulnérabilité.

5 Solution

Correctif disponible sur le site Microsoft :

<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=27500>

6 Documentation

Bulletin Microsoft :

<http://www.microsoft.com/technet/security/bulletin/MS01-006.asp>

Faq Microsoft :

<http://www.microsoft.com/technet/security/bulletin/fq01-006.asp>

Gestion détaillée du document

01 février 2001 version initiale.