

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le protocole RDP sous Windows 2000 et NT Server

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-126>

Gestion du document

Référence	CERTA-2001-AVI-126
Titre	Vulnérabilité dans le protocole RDP sous Windows 2000 et NT Server
Date de la première version	24 octobre 2001
Date de la dernière version	–
Source(s)	Bulletin Microsoft MS01-052
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.

2 Systèmes affectés

- Microsoft Windows 2000 Server ;
- Microsoft Windows 2000 Advanced Server ;
- Microsoft Windows 2000 Datacenter Server ;
- Microsoft Windows NT Server 4.0 ;
- Microsoft Windows NT Terminal Server Edition.

3 Résumé

Une vulnérabilité dans le protocole RDP permet à un utilisateur mal intentionné de réaliser 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.

Nota : Il n'est pas nécessaire de s'authentifier avec le serveur pour exploiter cette vulnérabilité. Seul l'envoi des paquets mal formés sur le port RDP (port TCP 3389) suffit.

5 Contournement provisoire

N'autoriser le trafic vers les ports RDP des serveurs qu'aux terminaux légitimes.

6 Solution

Télécharger le correctif concernant votre système sur le site Microsoft :

- Windows NT Server 4.0 et Terminal Serveur Edition :
<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=33250>
- Windows 2000 Server et Advanced Server :
<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=33389>

7 Documentation

Bulletin Microsoft :
<http://www.microsoft.com/technet/security/bulletin/MS01-052.asp>

Gestion détaillée du document

24 octobre 2001 version initiale.