

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité du protocole RDP de Microsoft

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-ALE-006>

Gestion du document

Référence	CERTA-2005-ALE-006-001
Titre	Vulnérabilité du protocole RDP de Microsoft
Date de la première version	18 juillet 2005
Date de la dernière version	10 août 2005
Source(s)	Avis de sécurité 904797 de Microsoft du 16 juillet 2005
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 avec Service Pack 4 ;
- Microsoft Windows XP ;
- Microsoft Windows XP avec SP 1 ;
- Microsoft Windows XP avec SP2 ;
- Microsoft Windows XP Professional ;
- Microsoft Windows XP édition Media Center (tout Service Pack) ;
- Microsoft Windows Server 2003 (tout Service Pack).

Le service vulnérable RDP (Bureau Distant ou Remote Desktop) est activé par défaut dans Windows XP Media Center.

3 Résumé

Microsoft a émis un avis de sécurité concernant une vulnérabilité dans le protocole RDP (Remote Desktop Protocol) qui peut provoquer un déni de service.

4 Description

Le protocole RDP (Remote Desktop Protocol) permet à un utilisateur d'établir une session virtuelle graphique vers une autre machine. La vulnérabilité découverte permet à un utilisateur distant mal intentionné de provoquer un arrêt inopiné du système, par le biais d'une requête malicieusement construite.

Plusieurs de nos correspondants ont noté depuis quelques jours une augmentation du trafic lié au port 3389/TCP, celui qui est utilisé pour initier une connexion RDP et donc éventuellement exploiter la vulnérabilité. Il semble en outre que les pare-feux intégrés dans plusieurs des systèmes d'exploitation vulnérables soient configurés par défaut pour laisser passer le trafic lié au protocole RDP.

5 Contournement provisoire

- Filtrer les paquets à destination du port 3389/TCP en provenance de l'Internet ;
- activer le filtrage du port 3389/TCP sur les pare-feux individuels ;
- désactiver les `Terminal Services` ou le service `Remote Desktop` s'ils ne sont pas nécessaires ;
- sécuriser les connexions RDP en utilisant IPsec ou une autre technique de réseau privé virtuel (VPN).

6 Solution

Appliquer le correctif de Microsoft indiqué dans le bulletin MS05-041 (voir Documentation).

7 Documentation

- Avis de sécurité 904797 de Microsoft du 16 juillet 2005 :
<http://www.microsoft.com/technet/security/advisory/904797.msp>
- Bulletin de sécurité Microsoft MS05-041 du 09 août 2005 :
<http://www.microsoft.com/technet/security/bulletin/MS05-041.msp>
- Avis CERTA-2005-AVI-304 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-304/index.html>
- Référence CVE CAN-2005-1218 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1218>

Gestion détaillée du document

18 juillet 2005 version initiale.

10 août 2005 ajout références avis Microsoft, avis CERTA et CVE. Ajout solution. Modification du résumé.