Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 août 2009
N° CERTA-2009-AVI-332

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans la Connexion Bureau à distance Microsoft

Gestion du document

Référence	CERTA-2009-AVI-332
Titre	Multiples vulnérabilités dans la Connexion Bureau à distance Microsoft
Date de la première version	12 août 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS09-044 du 11 août 2009
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

Exécution de code arbitraire à distance.

2 Systèmes affectés

- Microsoft RDP version 5.0 ;
- Microsoft RDP version 5.1 ;
- Microsoft RDP version 5.2 ;
- Microsoft RDP version 6.0 ;
- Microsoft RDP version 6.1.

Le Client Connexion Bureau à distance pour Mac 2.0 est également affecté.

3 Résumé

Deux vulnérabilités ont été identifiées dans la Connexion Bureau à distance de Microsoft (ou *Remote Desktop Protocol*, RDP). Ces vulnérabilités pourraient permettre l'exécution de code à distance si un attaquant parvenait à persuader un utilisateur des Services de terminaux (Terminal Services) de se connecter à un serveur RDP malveillant ou si un utilisateur visitait un site Web spécialement conçu.

4 Description

Deux vulnérabilités ont été identifiées dans la Connexion Bureau à distance de Microsoft. La première provient du fait que les paramètres renvoyés par le serveur RDP ne sont pas correctement traités. La seconde concerne le contrôle ActiveX du client. Dans les deux cas, seuls les clients RDP sont donc affectés.

Ces vulnérabilités pourraient permettre l'exécution de code à distance si un attaquant parvenait à persuader un utilisateur des Services de terminaux (Terminal Services) de se connecter à un serveur RDP malveillant ou si un utilisateur visitait un site Web spécialement conçu.

5 Solution

Se référer au bulletin de sécurité MS09-044 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS09-044 du 11 août 2009 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS09-044.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS09-044.mspx
- Référence CVE CVE-2009-1133 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1133
- Référence CVE CVE-2009-1929 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1929

Gestion détaillée du document

12 août 2009 version initiale.