



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 août 2011
N° CERTA-2011-AVI-441

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans la protocole RDP de Microsoft Windows

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-2011-AVI-441>

Gestion du document

Référence	CERTA-2011-AVI-441
Titre	Vulnérabilité dans la protocole RDP de Microsoft Windows
Date de la première version	10 août 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS-11-065 du 09 août 2011
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 à distance.

2 Systèmes affectés

- Windows XP Service Pack 3 ;
- Windows XP Professionnel Édition x64 Service Pack 2 ;
- Windows Server 2003 Service Pack 2 ;
- Windows Server 2003 Édition x64 Service Pack 2 ;
- Windows Server 2003 avec SP2 pour systèmes Itanium.

3 Résumé

Un vulnérabilité permettant à une personne malintentionnée d'effectuer un déni de service distant a été découverte dans le protocole *Bureau à distance* (RDP) de *Windows*.

4 Description

Une vulnérabilité existe dans le protocole *Bureau à distance* de *Windows*. Elle permet à une personne malintentionnée de causer un déni de service à distance grâce à l'envoi de paquets RDP spécialement conçus.

Cette faille est d'ores et déjà utilisée dans le cadre d'attaques ciblées.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS11-065 du 09 août 2011 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS11-065.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS11-065.msp>
- Référence CVE CVE-2011-1968 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1968>

Gestion détaillée du document

10 août 2011 version initiale.