Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 avril 2012
N° CERTA-2012-ALE-002-001

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité dans Windows RDP

Gestion du document

Référence	CERTA-2012-ALE-002-001
Titre	Vulnérabilité dans Windows RDP
Date de la première version	14 mars 2012
Date de la dernière version	13 avril 2012
Source	Bulletin de sécurité Microsoft MS12-020 du 13 mars 2012
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

- Windows XP SP3 ;
- Windows XP Professional édition x64 Service Pack 2 ;
- Windows Server 2003 Service Pack 2 ;
- Windows Server 2003 édition x64 Service Pack 2 ;
- Windows Server 2003 SP2 pour systèmes Itanium ;
- Windows Vista Service Pack 2 ;
- Windows Vista édition x64 Service Pack 2 ;
- Windows Server 2008 pour systèmes 32 bits Service Pack 2 ;
- Windows Server 2008 pour systèmes x64 Service Pack 2 ;
- Windows Server 2008 pour systèmes Itanium Service Pack 2 ;
- Windows 7 pour systèmes 32 et 64 bits ;
- Windows 7 pour systèmes 32 et 64 bits Service Pack 1 ;
- Windows Server 2008 R2 ;

- Windows Server 2008 R2 Service Pack 1 ;
- Windows Server 2008 R2 pour systèmes Itanium ;
- Windows Server 2008 R2 pour systèmes Itanium Service Pack 1.

3 Résumé

Une vulnérabilité affectant l'implémentation du protocole RDP sur la plupart des versions de Microsoft Windows a été corrigée. Elle permet à un attaquant distant d'exécuter du code arbitraire à distance.

4 Description

Le CERTA n'a pas connaissance à ce jour d'exploitation massive de cette vulnérabilité. Néanmoins, le CERTA alerte sur le caractère exceptionnel de sa criticité :

- le service RDP est très souvent activé comme moyen d'accès et d'administration de postes et de serveurs Windows à distance ;
- la vulnérabilité permet à un attaquant distant et anonyme d'exécuter du code arbitraire à distance.
- force est de constater que les services RDP sont largement exposés (et donc vulnérables) sur un réseau interne d'entreprise.

Les bonnes pratiques interdisent l'ouverture de ce service sur l'Internet, mais des listes publiques de serveurs RDP montrent que ces pratiques ne sont pas toujours respectées.

Il est donc primordial d'appliquer sans délai le correctif fourni par Microsoft, et de s'assurer que les services RDP ne sont accessibles que depuis des postes bien identifiés.

5 Solution

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

6 Documentation

- Bloc-notes Microsoft Security Research & Defense CVE-2012-0002 :
  http://blogs.technet.com/b/srd/archive/2012/03/13/cve-2012-0002-a-closer-look-at-ms12-020-s-critical-issue.aspx
- Bulletin de sécurité Microsoft MS12-020 du 13 mars 2012 :
  http://technet.microsoft.com/fr-fr/security/bulletin/MS12-020
  http://technet.microsoft.com/en-us/security/bulletin/MS12-020
- Référence CVE CVE-2012-0002 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0002

Gestion détaillée du document

14 mars 2012 version initiale.
13 avril 2012 explicitation du correctif éditeur comme solution.