Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 août 2012
N° CERTA-2012-AVI-437

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans les composants réseau Microsoft Windows

Gestion du document

Référence	CERTA-2012-AVI-437
Titre	Multiples vulnérabilités dans les composants réseau Microsoft Windows
Date de la première version	16 août 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité MS12-054 du 14 août 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 ;
- déni de service à distance.

2 Systèmes affectés

- Windows XP Service Pack 3 ;
- Windows XP Professionnel x64 Service Pack 2 ;
- Windows Server 2003 Service Pack 2 ;
- Windows Server 2003 Service x64 Pack 2 ;
- Windows Server 2003 Itanium Service Pack 2 ;
- Windows Vista Service Pack 2 ;
- Windows Vista x64 Service Pack 2 ;
- Windows Server 2008 Service Pack 2 ;
- Windows Server 2008 x64 Service Pack 2 ;
- Windows Server 2008 Itanium Service Pack 2 ;
- Windows 7 ;
- Windows 7 Service Pack 1 ;

- Windows 7 x64 ;
- Windows 7 x64 Service Pack 1 ;
- Windows Server 2008 R2 x64 ;
- Windows Server 2008 R2 x64 Service Pack 1 ;
- Windows Server 2008 R2 Itanium ;
- Windows Server 2008 R2 Itanium Service Pack 1.

3 Résumé

Quatre vulnérabilités ont été corrigées dans les composants de *Microsoft Windows*. Une faille de type « format string » affecte le service d'impression. Les trois autres concernent le protocole d'administration à distance : deux débordements de mémoire tampon (un sur la pile et un dans le tas) et un déni de service.

4 Solution

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

5 Documentation

- Bulletin de sécurité Microsoft MS12-054 du 14 août 2012 :
  http://technet.microsoft.com/fr-fr/security/bulletin/MS12-054
  http://technet.microsoft.com/en-us/security/bulletin/MS12-054
- Référence CVE CVE-2012-1850 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1850
- Référence CVE CVE-2012-1851 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1851
- Référence CVE CVE-2012-1852 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1852
- Référence CVE CVE-2012-1853 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1853

Gestion détaillée du document

14 août 2012 version initiale.