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 juillet 2013
N° CERTA-2013-AVI-399

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans le noyau Microsoft Windows

Gestion du document

Référence	CERTA-2013-AVI-399
Titre	Multiples vulnérabilités dans le noyau Microsoft Windows
Date de la première version	10 juillet 2013
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft du 09 juillet 2013
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(s)

- exécution de code arbitraire à distance
- élévation de privilèges

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
- 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 bits Service Pack 1
- Windows 7 pour systèmes x64 Service Pack 1

- Windows Server 2008 R2 pour systèmes x64 Service Pack 1
- Windows Server 2008 R2 pour systèmes Itanium Service Pack 1
- Windows 8 pour systèmes 32 bits
- Windows 8 pour systèmes 64 bits
- Windows Server 2012
- Windows RT

3 Résumé

De multiples vulnérabilités ont été corrigées dans *le noyau Microsoft Windows*. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance et une élévation de privilèges.

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 MS13-053 du 09 juillet 2013
  http://technet.microsoft.com/en-us/security/bulletin/MS13-053
- Référence CVE CVE-2013-1300
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1300
- Référence CVE CVE-2013-1340
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1340
- Référence CVE CVE-2013-1345
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1345
- Référence CVE CVE-2013-3129
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3129
- Référence CVE CVE-2013-3167
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3167
- Référence CVE CVE-2013-3172
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3172
- Référence CVE CVE-2013-3173
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3173
- Référence CVE CVE-2013-3660
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3660

Gestion détaillée du document

10 juillet 2013 version initiale.