

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans le noyau Windows (win32k.sys)

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-2012-AVI-325>

Gestion du document

Référence	CERTA-2012-AVI-325
Titre	Multiples vulnérabilités dans le noyau Windows (win32k.sys)
Date de la première version	13 juin 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS12-041 du 12 juin 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

Élévation de privilèges.

2 Systèmes affectés

- Windows XP Service Pack 3 ;
- Windows XP Professional x64 Edition Service Pack 2 ;
- Windows Server 2003 Service Pack 2 ;
- Windows Server 2003 x64 Edition Service Pack 2 ;
- Windows Server 2003 SP2 pour les systèmes Itanium ;
- Windows Vista Service Pack 2 ;
- Windows Vista x64 Edition Service Pack 2 ;
- Windows Server 2008 32-bit Service Pack 2 ;
- Windows Server 2008 x64 Service Pack 2 ;
- Windows Server 2008 Itanium Service Pack 2 ;
- Windows 7 32-bit ;
- Windows 7 32-bit 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

Cinq vulnérabilités ont été corrigées dans le noyau *Microsoft Windows*. Elles permettent toutes une élévation de privilèges. Trois concernent « Atom », une est un débordement d'entier lors de l'allocation des polices de caractères et la dernière intervient lors de demandes concurrentes à la création d'un *thread*.

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 MS12-041 du 12 juin 2012 :
<http://technet.microsoft.com/fr-fr/security/bulletin/MS12-041>
<http://technet.microsoft.com/en-us/security/bulletin/MS12-041>
- Référence CVE CVE-2012-1864 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1864>
- Référence CVE CVE-2012-1865 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1865>
- Référence CVE CVE-2012-1866 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1866>
- Référence CVE CVE-2012-1867 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1867>
- Référence CVE CVE-2012-1868 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1868>

Gestion détaillée du document

13 juin 2012 version initiale.