Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 11 juillet 2012
N° CERTA-2012-AVI-379

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans des pilotes du noyau Windows

Gestion du document

Référence	CERTA-2012-AVI-379
Titre	Vulnérabilités dans des pilotes du noyau Windows
Date de la première version	11 juillet 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS12-047 du 10 juillet 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 ;
- élévation de privilèges.

2 Systèmes affectés

- Windows XP Service Pack 3 ;
- Windows XP Professionnel Edition x64 Service Pack 2 ;
- Windows Server 2003 Service Pack 2 ;
- Windows Server 2003 Edition x64 Service Pack 2 ;
- Windows Server 2003 Service Pack 2 pour systèmes Itanium ;
- Windows Vista Service Pack 2 ;
- Windows Vista Edition 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 ;
- Windows 7 pour systèmes 32 bits Service Pack 1 ;

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

3 Résumé

Deux vulnérabilités ont été corrigées dans des pilotes du noyau de *windows*. La première (CVE-2012-1890) concerne le pilote de gestion du clavier qui ne gère pas correctement certaines configurations. La seconde (CVE-2012-1893) est due à une mauvaise validation de certains paramètres lors de la création d'une procédure de *hook*. Dans les deux cas, un utilisateur malintentionné peut utiliser ces vulnérabilités afin d'exécuter du code arbitraire avec des droits élevés.

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 MS12-047 du 10 juillet 2012 :
  http://technet.microsoft.com/fr-fr/security/bulletin/MS12-047
  http://technet.microsoft.com/en-us/security/bulletin/MS12-047
- Référence CVE CVE-2012-1890 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1890
- Référence CVE CVE-2012-1893 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1893

Gestion détaillée du document

11 juillet 2012 version initiale.