



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 juillet 2011
N° CERTA-2011-AVI-388

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans les pilotes en mode noyau du système Microsoft Windows

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-2011-AVI-388>

Gestion du document

Référence	CERTA-2011-AVI-388
Titre	Vulnérabilités dans les pilotes en mode noyau du système Microsoft Windows
Date de la première version	13 juillet 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS11-054 du 12 juillet 2011
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 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 1 et Windows Vista Service Pack 2 ;
- Windows Vista Édition x64 Service Pack 1 et Windows Vista Édition x64 Service Pack 2 ;
- Windows Server 2008 pour systèmes 32 bits et Windows Server 2008 pour systèmes 32 bits Service Pack 2* ;
- Windows Server 2008 pour systèmes x64 et Windows Server 2008 pour systèmes x64 Service Pack 2* ;
- Windows Server 2008 pour systèmes Itanium et Windows Server 2008 pour systèmes Itanium Service Pack 2 ;
- Windows 7 pour systèmes 32 bits et Windows 7 pour systèmes 32 bits Service Pack 1 ;

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

3 Résumé

Plusieurs vulnérabilités dans les pilotes en mode noyau de Microsoft Windows peuvent être exploitées par un utilisateur local authentifié afin d'élever ses privilèges.

4 Description

De multiples vulnérabilités ont été corrigées dans la façon dont les pilotes en mode noyau de Microsoft Windows gèrent et assurent le suivi des objets de pilote. Ces vulnérabilités peuvent permettre à un utilisateur local authentifié d'élever ses privilèges.

5 Solution

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

6 Documentation

- Bulletin de sécurité Microsoft MS11-054 du 12 juillet 2011 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS11-054.mspx>
<http://www.microsoft.com/technet/security/Bulletin/MS11-054.mspx>
- Référence CVE-2011-1874 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1874>
- Référence CVE-2011-1875 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1875>
- Référence CVE-2011-1876 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1876>
- Référence CVE-2011-1877 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1877>
- Référence CVE-2011-1878 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1878>
- Référence CVE-2011-1879 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1879>
- Référence CVE-2011-1880 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1880>
- Référence CVE-2011-1881 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1881>
- Référence CVE-2011-1882 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1882>
- Référence CVE-2011-1883 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1883>
- Référence CVE-2011-1884 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1884>
- Référence CVE-2011-1885 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1885>
- Référence CVE-2011-1886 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1886>

- Référence CVE-2011-1887 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1887>
- Référence CVE-2011-1888 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1888>

Gestion détaillée du document

13 juillet 2011 version initiale.