



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 avril 2011
N° CERTA-2011-AVI-217

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans des 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-217>

Gestion du document

Référence	CERTA-2011-AVI-217
Titre	Multiples vulnérabilités dans des pilotes en mode noyau du système Microsoft Windows
Date de la première version	13 avril 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS11-034
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

- Microsoft Windows XP Service Pack 3 ;
- Microsoft Windows XP Professionnel Édition x64 Service Pack 2 ;
- Microsoft Windows Server 2003 Service Pack 2 ;
- Microsoft Windows Server 2003 Édition x64 Service Pack 2 ;
- Microsoft Windows Vista Service Pack 1 et Service Pack 2 ;
- Microsoft Windows Vista Édition x64 Service Pack 1 et Service Pack 2 ;
- Microsoft Windows Server 2008 pour systèmes 32 bits ;
- Microsoft Windows Server 2008 pour systèmes 32 bits Service Pack 2 ;
- Microsoft Windows Server 2008 pour systèmes x64 ;
- Microsoft Windows Server 2008 pour systèmes x64 Service Pack 2 ;
- Microsoft Windows Server 2008 pour systèmes Itanium ;
- Microsoft Windows Server 2008 pour systèmes Itanium Service Pack 2 ;

- Microsoft Windows 7 pour systèmes 32 bits ;
- Microsoft Windows 7 pour systèmes 32 bits Service Pack 1 ;
- Microsoft Windows 7 pour systèmes x64 ;
- Microsoft Windows 7 pour systèmes x64 Service Pack 1 ;
- Microsoft Windows Server 2008 R2 pour systèmes x64 ;
- Microsoft Windows Server 2008 R2 pour systèmes x64 Service Pack 1 ;
- Microsoft Windows Server 2008 R2 pour systèmes Itanium ;
- Microsoft Windows Server 2008 R2 pour systèmes Itanium Service Pack 1.

3 Résumé

Deux vulnérabilités affectant le sous-système *win32k* des systèmes Microsoft Windows ont été découvertes. Celles-ci permettent à un utilisateur local authentifié d'élever ses privilèges.

4 Description

Ces deux vulnérabilités affectent le sous-système *win32k* des environnements Microsoft Windows. Un utilisateur malveillant authentifié localement sur le poste peut se servir de celles-ci pour élever son niveau de privilège. La première faille de sécurité se situe dans la manière avec laquelle les pilotes Windows en mode noyau gèrent leurs objets chargés en mode noyau. La seconde est localisée dans la gestion des pointeurs vers des objets en mode noyau utilisés par ces mêmes pilotes.

Les 30 références CVE listées ci-dessous ont toutes pour cause initiale une de ces deux vulnérabilités, appliquées à différents objets du noyau.

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 MS11-034 du 13 avril 2011 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS11-034.mspx>
<http://www.microsoft.com/technet/security/Bulletin/MS11-034.mspx>
- Référence CVE CVE-2011-0662 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0662>
- Référence CVE CVE-2011-0665 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0665>
- Référence CVE CVE-2011-0666 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0666>
- Référence CVE CVE-2011-0667 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0667>
- Référence CVE CVE-2011-0670 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0670>
- Référence CVE CVE-2011-0671 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0671>
- Référence CVE CVE-2011-0672 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0672>
- Référence CVE CVE-2011-0673 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0673>
- Référence CVE CVE-2011-0674 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0674>
- Référence CVE CVE-2011-0675 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0675>

- Référence CVE CVE-2011-0676 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0676>
- Référence CVE CVE-2011-0677 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0677>
- Référence CVE CVE-2011-1225 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1225>
- Référence CVE CVE-2011-1226 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1226>
- Référence CVE CVE-2011-1227 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1227>
- Référence CVE CVE-2011-1228 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1228>
- Référence CVE CVE-2011-1229 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1229>
- Référence CVE CVE-2011-1230 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1230>
- Référence CVE CVE-2011-1231 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1231>
- Référence CVE CVE-2011-1232 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1232>
- Référence CVE CVE-2011-1233 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1233>
- Référence CVE CVE-2011-1234 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1234>
- Référence CVE CVE-2011-1235 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1235>
- Référence CVE CVE-2011-1236 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1236>
- Référence CVE CVE-2011-1237 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1237>
- Référence CVE CVE-2011-1238 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1238>
- Référence CVE CVE-2011-1239 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1239>
- Référence CVE CVE-2011-1240 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1240>
- Référence CVE CVE-2011-1241 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1241>
- Référence CVE CVE-2011-1242 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1242>

Gestion détaillée du document

13 avril 2011 version initiale.