

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité 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-349>

Gestion du document

| | |
|-----------------------------|---|
| Référence | CERTA-2011-AVI-349 |
| Titre | Vulnérabilité dans les pilotes en mode noyau du système Microsoft Windows |
| Date de la première version | 15 juin 2011 |
| Date de la dernière version | – |
| Source(s) | Bulletin de sécurité Microsoft MS11-041 du 14 juin 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

- Exécution de code arbitraire à distance ;
- élévation de privilèges.

2 Systèmes affectés

- Windows XP Professionnel Édition x64 SP2 ;
- Windows Server 2003 Édition x64 SP2 ;
- Windows Vista Édition x64 SP1 et Windows Vista Édition x64 SP2 ;
- Windows Server 2008 pour systèmes Itanium et Windows Server 2008 pour systèmes Itanium SP2 ;
- Windows 7 pour systèmes x64 et Windows 7 pour systèmes x64 SP1 ;
- Windows Server 2008 R2 pour systèmes x64 et Windows Server 2008 R2 pour systèmes x64 SP1 ;
- Windows Server 2008 R2 pour systèmes Itanium et Windows Server 2008 R2 pour systèmes Itanium SP1.

3 Résumé

Une vulnérabilité dans les pilotes en mode noyau de Windows a été identifiée. Cette vulnérabilité peut être utilisée par une personne malveillante distante pour élever ses privilèges ou provoquer de l'exécution de code arbitraire.

4 Description

Une vulnérabilité liée au traitement des polices *OpenType* par les pilotes en mode noyau de Windows a été corrigée. Cette vulnérabilité peut être exploitée par une personne malveillante distante, pour provoquer de l'exécution de code arbitraire ou élever ses privilèges, en dirigeant un utilisateur vers un partage réseau contenant une police *OpenType* spécialement conçue.

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 MS11-041 du 14 juin 2011 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS11-041.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS11-041.msp>
- Référence CVE CVE-2011-1873 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1873>

Gestion détaillée du document

15 juin 2011 version initiale.