



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 octobre 2010
N° CERTA-2010-AVI-483

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans les pilotes en mode noyau de 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-2010-AVI-483>

Gestion du document

Référence	CERTA-2010-AVI-483
Titre	Vulnérabilités dans les pilotes en mode noyau de Windows
Date de la première version	13 octobre 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS10-073 du 12 octobre 2010
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 1 et Windows Vista Service Pack 2 ;
- Windows Vista x64 Edition Service Pack 1 et Windows Vista x64 Edition Service Pack 2 ;
- Windows Server 2008 pour les systèmes 32 bits, 64 bits ou Itanium, avec ou sans le Service Pack 2 ;
- Windows 7 pour les systèmes 32 bits et 64 bits ;
- Windows Server 2008 R2 pour les systèmes 64 bits ou Itanium.

3 Résumé

Une vulnérabilité affectant la gestion des pilotes en mode noyau permet une élévation de privilèges. Ce bulletin remplace le MS10-048 du 10 août 2010.

4 Description

Une vulnérabilité affecte la gestion des pilotes en mode noyau. Elle est due à un défaut de gestion d'index et permet à une personne malintentionnée, possédant déjà un accès sur le système, d'élever ses droits. Ce bulletin remplace le MS10-048 publié le 10 août 2010.

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 MS10-073 du 12 octobre 2010 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS10-073.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS10-073.msp>
- Référence CVE CVE-2010-2549 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2549>
- Référence CVE CVE-2010-2743 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2743>
- Référence CVE CVE-2010-2744 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2744>

Gestion détaillée du document

13 octobre 2010 version initiale.