



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 février 2007
N° CERTA-2007-AVI-079

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du service Microsoft de détection matériel noyau

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-2007-AVI-079>

Gestion du document

Référence	CERTA-2007-AVI-079
Titre	Vulnérabilité du service Microsoft de détection matériel noyau
Date de la première version	14 février 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS07-006 du 13 février 2007
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

- Contournement de la politique de sécurité ;
- élévation de privilèges.

2 Systèmes affectés

- Microsoft Windows XP Service Pack 2 ;
- Microsoft Windows XP Professional x64 Edition ;
- Microsoft Windows Server 2003, y compris le Service Pack 1 ;
- Microsoft Windows Server 2003, y compris le Service Pack 1, pour les systèmes Itanium ;
- Microsoft Windows Server 2003 x64 Edition.

3 Description

Une vulnérabilité a été identifiée dans le service de détection matériel noyau (ou Shell Hardware Detection) de Microsoft Windows. Celui-ci, démarré automatiquement par défaut, fournit des signalements aux événements matériel de lecture automatique (Autoplay hardware).

Un paramètre ne serait pas correctement vérifié au moment où le matériel commence à interagir avec Microsoft Windows. Une personne malveillante, disposant d'une session sur la machine, peut exploiter cette vulnérabilité localement, par exemple par le biais d'une application, afin d'élever ses privilèges à ceux de l'administrateur. Il serait également possible d'exploiter cette vulnérabilité sous forme d'un *Cheval de Troie*.

4 Solution

Se référer au bulletin de sécurité MS07-006 de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

5 Documentation

- Bulletin de sécurité Microsoft MS07-006 du 13 février 2007 :
<http://www.microsoft.com/france/technet/security/bulletin/MS07-006.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS07-006.msp>
- Référence CVE CVE-2007-0211 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0211>

Gestion détaillée du document

14 février 2007 version initiale.