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-080

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de l'Acquisition d'Image Windows (WIA)

Gestion du document

Référence	CERTA-2007-AVI-080
Titre	Vulnérabilité de l'Acquisition d'Image Windows (WIA)
Date de la première version	14 février 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS07-007 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 SP 2.

3 Description

Une vulnérabilité, de type débordement de mémoire tampon, a été identifiée dans le service d'`Acquisition d'Image Windows (WIA)` (ou *Windows Image Acquisition*) de Microsoft Windows. Ce service démarre manuellement. Il sert d'interface entre les applications logicielles (Adobe Photoshop par exemple) et les matériels multimédia, tels que les appareils photo numériques, les scanners, ou les *webcams*.

Une personne malveillante, disposant d'une session sur la machine vulnérable, peut lancer une application exploitant cette vulnérabilité, afin d'élever ses privilèges à ceux de l'administrateur. Il serait également possible d'exploiter cette vulnérabilité par le biais d'un *Cheval de Troie*.

4 Solution

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

5 Documentation

- Bulletin de sécurité Microsoft MS07-007 du 13 février 2007 :
  http://www.microsoft.com/france/technet/security/bulletin/MS07-007.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS07-007.mspx
- Référence CVE CVE-2007-0210 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0210

Gestion détaillée du document

14 février 2007 version initiale.