Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 11 août 2010
N° CERTA-2010-AVI-364

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités de pilotes en mode noyau de Windows

Gestion du document

Référence	CERTA-2010-AVI-364
Titre	Vulnérabilités de pilotes en mode noyau de Windows
Date de la première version	11 août 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS10-048 du 10 août 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

- Déni de service ;
- élévation de privilèges.

2 Systèmes affectés

Windows, toutes versions, toutes éditions.

3 Résumé

Plusieurs vulnérabilités affectent les pilotes en mode noyau de Windows. Leur exploitation permet à un utilisateur local malveillant de réaliser un déni de service ou d'élever ses privilèges.

4 Description

Plusieurs vulnérabilités affectent les pilotes en mode noyau de Windows :

- (CVE-2010-1887) lors d'un appel système, des paramètres transmis ne sont pas validés correctement. Ce défaut est exploitable par un utilisateur malveillant pour réaliser un déni de service ;

- (CVE-2010-1894) une erreur dans le traitement des exceptions est exploitable par un utilisateur malveillant pour élever ses privilèges ;
- (CVE-2010-1895) les pilotes en mode noyau allouent de manière incorrecte de la mémoire dans certaines circonstances. Ce problème est exploitable par un utilisateur malveillant pour élever ses privilèges ;
- (CVE-2010-1896) des entrées transmises depuis le mode utilisateur ne sont pas validées correctement. Ce problème est exploitable par un utilisateur malveillant pour élever ses privilèges ;
- (CVE-2010-1897) des paramètres ne sont pas validées correctement lors de la création de fenêtres par les pilotes. Ce problème est exploitable par un utilisateur malveillant pour élever ses privilèges.

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 MS10-048 du 10 août 2010 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS10-048.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS10-048.mspx
- Référence CVE CVE-2010-1887 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1887
- Référence CVE CVE-2010-1894 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1894
- Référence CVE CVE-2010-1895 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1895
- Référence CVE CVE-2010-1896 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1896
- Référence CVE CVE-2010-1897 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1897

Gestion détaillée du document

11 août 2010 version initiale.