

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans le noyau 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-169>

Gestion du document

Référence	CERTA-2010-AVI-169
Titre	Vulnérabilités dans le noyau Windows
Date de la première version	14 avril 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS10-021 du 13 avril 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

- Dénis de service ;
- élévation de privilèges.

2 Systèmes affectés

Windows, toutes les versions, toutes les architectures.

3 Résumé

Plusieurs vulnérabilités affectant le noyau Windows ont été publiées. Leur exploitation permet à un utilisateur malveillant de provoquer un déni de service ou d'élever ses privilèges.

4 Description

Plusieurs vulnérabilités affectant le noyau Windows ont été publiées :

- deux erreurs dans le traitement des clefs de registre sont utilisables par un utilisateur malveillant pour provoquer le redémarrage du système ;

- une erreur dans le traitement des liens symboliques est utilisable par un utilisateur malveillant pour provoquer le redémarrage du système ;
- deux erreurs lors du traitement de certaines clefs de registre permettent à un utilisateur malveillant d'exécuter du code arbitraire avec les droits du noyau ;
- une erreur dans la conversion des chemins virtuels en chemin réels pour les clefs de registre est utilisable par un utilisateur malveillant pour provoquer le redémarrage du système ;
- une erreur dans le traitement des fichiers images est utilisable par un utilisateur malveillant pour provoquer le redémarrage du système ;
- une erreur dans le traitement des exceptions est utilisable par un utilisateur malveillant pour provoquer le redémarrage du système.

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 MS10-021 du 13 avril 2010 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS10-021.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS10-021.msp>
- Référence CVE CVE-2010-0234 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0234>
- Référence CVE CVE-2010-0235 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0235>
- Référence CVE CVE-2010-0236 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0236>
- Référence CVE CVE-2010-0237 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0237>
- Référence CVE CVE-2010-0238 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0238>
- Référence CVE CVE-2010-0481 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0481>
- Référence CVE CVE-2010-0482 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0482>
- Référence CVE CVE-2010-0810 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0810>

Gestion détaillée du document

14 avril 2010 version initiale.