

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-363>

Gestion du document

Référence	CERTA-2010-AVI-363
Titre	Vulnérabilités dans le noyau Windows
Date de la première version	11 août 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS10-047 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

- Exécution de code arbitraire ;
- déni de service ;
- élévation de privilèges.

2 Systèmes affectés

- Windows XP SP3 ;
- Windows Vista, toutes éditions ;
- Windows 7, toutes éditions ;
- Windows Server 2008, toutes éditions.

3 Résumé

Plusieurs vulnérabilités affectent le noyau du système d'exploitation Windows. Leur exploitation permet à un utilisateur local de réaliser un déni de service, d'élever ses privilèges ou d'exécuter du code arbitraire.

4 Description

Plusieurs vulnérabilités affectent le noyau du système d'exploitation Windows :

- (CVE-2010-1888) un défaut du noyau de Windows XP SP3 concerne la tentative de création de certains fils d'exécution (*threads*). Son exploitation permet à un utilisateur local d'élever ses privilèges et d'exécuter du code arbitraire ;
- (CVE-2010-1889) une erreur dans la libération de mémoire par le noyau lors du traitement de certaines erreurs permet à un utilisateur local d'élever ses privilèges et d'exécuter du code arbitraire ;
- (CVE-2010-1890) un problème dans la validation des listes de contrôle d'accès aux objets du noyau par le noyau permet à un utilisateur local d'empêcher le système de répondre ou de le forcer à redémarrer.

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 MS10-047 du 10 août 2010 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS10-047.aspx>
<http://www.microsoft.com/technet/security/Bulletin/MS10-047.aspx>
- Référence CVE CVE-2010-1888 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1888>
- Référence CVE CVE-2010-1889 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1889>
- Référence CVE CVE-2010-1890 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1890>

Gestion détaillée du document

11 août 2010 version initiale.