

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans le noyau de Microsoft 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-2009-AVI-492>

Gestion du document

Référence	CERTA-2009-AVI-492
Titre	Vulnérabilités dans le noyau de Microsoft Windows
Date de la première version	10 novembre 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS09-065 du 10 novembre 2009
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 à distance ;
- élévation de privilèges.

2 Systèmes affectés

- *Microsoft Windows 2000* SP4 ;
- *Microsoft Windows XP* SP2 et SP3, toutes versions et architectures ;
- *Microsoft Windows Server 2003*, toutes versions et architectures ;
- *Microsoft Windows Vista*, y compris SP1 et SP2, toutes versions et architectures ;
- *Microsoft Windows Server 2008*, y compris SP2, toutes versions et architectures.

Note : *Microsoft Windows Server 2008* R2 n'est pas vulnérable.

3 Résumé

Plusieurs vulnérabilités du noyau de *Microsoft Windows* permettent à un utilisateur malveillant d'élever ses privilèges ou d'exécuter du code arbitraire à distance.

4 Description

Trois vulnérabilités du noyau de *Microsoft Windows* ont été publiées :

- la mauvaise gestion d'un pointeur nul est exploitable par un utilisateur malintentionné pour exécuter du code arbitraire en mode noyau ;
- un manque de validation des données fournies par les pilotes des interfaces graphiques peut servir à un utilisateur malveillant pour élever ses privilèges et exécuter du code arbitraire en mode noyau ;
- un défaut d'analyse des polices de caractères est utilisable par un utilisateur malveillant pour exécuter en mode noyau du code arbitraire.

Ces vulnérabilités sont exploitables à distance avec le concours d'un utilisateur connecté, par exemple en l'incitant à consulter une page web spécialement conçue.

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 MS09-065 du 10 novembre 2009 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS09-065.mspx>
<http://www.microsoft.com/technet/security/Bulletin/MS09-065.mspx>
- Référence CVE CVE-2009-1127 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1127>
- Référence CVE CVE-2009-2513 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2513>
- Référence CVE CVE-2009-2514 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2514>

Gestion détaillée du document

10 novembre 2009 version initiale.