

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Microsoft Windows Shell et Web View

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-2005-AVI-401>

Gestion du document

| | |
|-----------------------------|---|
| Référence | CERTA-2005-AVI-401 |
| Titre | Multiples vulnérabilités dans Microsoft Windows Shell et Web View |
| Date de la première version | 12 octobre 2005 |
| Date de la dernière version | - |
| Source(s) | Bulletin de sécurité Microsoft MS05-049 du 11 octobre 2005 |
| 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.

2 Systèmes affectés

- Microsoft Windows 2000 Service Pack 4 ;
- Microsoft Windows XP Service Pack 1 & 2 ;
- Microsoft Windows XP Professionnal x64 Edition ;
- Microsoft Windows Server 2003 et Microsoft Windows Server 2003 Service Pack 1 ;
- Microsoft Windows Server 2003 et Microsoft Windows Server 2003 Service Pack 1 pour systèmes Itanium ;
- Microsoft Windows Server 2003 x64 Edition.

3 Résumé

De nombreuses vulnérabilités découvertes dans l'interpréteur de commande et dans l'application `Web view` de Microsoft permettent à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

4 Description

Deux vulnérabilités causées par une mauvaise gestion des fichiers `.lnk` permettent à une personne malveillante d'exécuter du code arbitraire à distance au moyen d'un site web contenant un fichier `.lnk` habilement construit.

Une erreur dans le traitement de certains caractères HTML permet à un individu mal intentionné d'exécuter du code arbitraire à distance au moyen d'un site web malicieusement construit.

5 Solution

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

6 Documentation

- Site Internet de l'éditeur :
<http://www.microsoft.com>
- Bulletin de sécurité Microsoft MS05-049 du 11 octobre 2005 :
<http://www.microsoft.com/technet/security/Bulletin/MS05-049.msp>
- Référence CVE CAN-2005-2117 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2117>
- Référence CVE CAN-2005-2118 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2117>
- Référence CVE CAN-2005-2122 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2122>

Gestion détaillée du document

12 octobre 2005 version initiale.