

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans la bibliothèque `hlink.dll` 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-2006-AVI-348>

Gestion du document

Référence	CERTA-2006-AVI-348
Titre	Multiples vulnérabilités dans la bibliothèque <code>hlink.dll</code> de Microsoft Windows
Date de la première version	09 août 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS06-050 du 08 août 2006
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 et 2 ;
- Microsoft Windows XP édition x64 ;
- Microsoft Windows Server 2003 ;
- Microsoft Windows Server 2003 Service Pack 1 ;
- Microsoft Windows Server 2003 pour Itanium ;
- Microsoft Windows Server 2003 pour Itanium Service Pack 1 ;
- Microsoft Windows Server 2003 édition x64.

3 Résumé

Deux vulnérabilités présentes dans la bibliothèque de fonctions `hlink.dll` de Microsoft Windows permettent à un utilisateur distant mal intentionné d'exécuter du code arbitraire.

4 Description

La bibliothèque de fonctions `hlink.dll` de Microsoft Windows permet la mise en œuvre de liens hypertexte dans différentes applications comme `Outlook` ou celles de la suite `Office`. Deux vulnérabilités présentes dans des fonctions de cette bibliothèque permettent à un utilisateur mal intentionné d'exécuter du code arbitraire par le biais d'un objet de type « lien hypertexte » construit de façon particulière. Cet objet peut être véhiculé via un message électronique ou bien via un document `Office` comme une feuille de calculs `Excel` par exemple.

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 MS06-050 du 08 août 2006 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS06-050.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS06-050.msp>
- Référence CVE CVE-2006-3086 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3086>
- Référence CVE CVE-2006-3438 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3438>

Gestion détaillée du document

09 août 2006 version initiale.