



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité
des systèmes d'information
CERTA

Paris, le 09 février 2005
N° CERTA-2005-AVI-056

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le traitement des hyperliens sous 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-2005-AVI-056>

Gestion du document

Référence	CERTA-2005-AVI-056
Titre	Vulnérabilité dans le traitement des hyperliens sous Windows
Date de la première version	09 février 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS05-015 du 08 février 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 3 et Service Pack 4 ;
- Microsoft Windows XP Service Pack 1 et Service Pack 2 ;
- Microsoft Windows XP 64-Bit Edition Service Pack 1 (Itanium) ;
- Microsoft Windows Server 2003 ;
- Microsoft Windows Server 2003 pour les systèmes Itanium.

3 Résumé

Une vulnérabilité dans le traitement des hyperliens permet l'exécution de code arbitraire à distance.

4 Description

Le traitement des hyperliens est assuré par la bibliothèque `hlink.dll` ou `whlink.dll` (en fonction de la version du système d'exploitation). Une vulnérabilité dans cette bibliothèque permet, par l'intermédiaire d'un lien habilement constitué (par exemple sur un site web ou dans un message électronique), l'exécution de code arbitraire à distance.

5 Contournement provisoire

Configurer les clients de messagerie pour lire les messages en texte brut (`plain text`), et ne naviguer que sur des sites de confiance.

6 Solution

Appliquer le correctif tel qu'indiqué dans le bulletin de sécurité Microsoft MS05-015 du 08 février 2005 (voir section Documentation).

7 Documentation

- Bulletin de sécurité Microsoft MS05-015 du 08 février 2005 :
<http://www.microsoft.com/technet/security/bulletin/ms05-015.msp>
- Référence CVE CAN-2005-057 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0053>

Gestion détaillée du document

09 février 2005 version initiale.