



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 11 mai 2005
N° CERTA-2005-AVI-162

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de l'explorateur 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-162>

Gestion du document

Référence	CERTA-2005-AVI-162
Titre	Vulnérabilité de l'explorateur Windows
Date de la première version	11 mai 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité MS05-024 de Microsoft
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

2 Systèmes affectés

- Microsoft Windows 2000 Service Pack 3 ;
- Microsoft Windows 2000 Service Pack 4 ;
- Microsoft Windows 98 ;
- Microsoft Windows 98 Second Edition ;
- Microsoft Windows Millenium Edition (ME).

3 Résumé

Une vulnérabilité dans la manière dont l'explorateur Windows gère certains caractères HTML permet l'exécution de code arbitraire lors de la prévisualisation d'un fichier malicieusement construit.

4 Description

Une vulnérabilité a été découverte dans le traitement des pages html par l'explorateur Windows et plus précisément leur prévisualisation avec la fonction *Affichage en Miniatures*.

En persuadant un utilisateur de prévisualiser un fichier malicieusement construit, un individu mal intentionné peut exécuter du code arbitraire avec les droits de l'utilisateur.

5 Contournement provisoire

Désactiver l'option *Affichage en Miniatures* de l'explorateur Windows.

6 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs.

7 Documentation

- Bulletin de sécurité de Microsoft MS05-24 du 10 mai 2005 :
<http://www.microsoft.com/technet/security/bulletin/MS05-024.mspx>
- Référence CVE CAN-2005-1191 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1191>

Gestion détaillée du document

11 mai 2005 version initiale.