



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-053

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le traitements des images PNG pour plusieurs applications Microsoft

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-053>

Gestion du document

Référence	CERTA-2005-AVI-053
Titre	Vulnérabilité dans le traitements des images PNG pour plusieurs applications Microsoft
Date de la première version	09 février 2005
Date de la dernière version	-
Source(s)	Bulletin de sécurité MS05-009 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 à distance.

2 Systèmes affectés

- Microsoft Windows Media Player 9.x (hors Windows XP SP2) ;
- Microsoft Windows Messenger 5.0 ;
- Microsoft Windows MSN Messenger 6.1, 6.2 ;
- Microsoft Windows 98, 98 (SE), Millennium Edition (ME).

3 Description

PNG ("Portable Network Graphics") est un format d'image utilisé par plusieurs application Windows telles la messagerie instantanée (MSN messenger) ou l'outil Media Player.

Plusieurs vulnérabilités ont été découvertes lors du traitement de fichiers au format PNG. Au moyen d'un fichier PNG habilement constitué, un utilisateur mal intentionné peut réaliser l'exécution de code arbitraire à travers l'application vulnérable sur la plate-forme client.

4 Solution

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

5 Documentation

- Bulletin de sécurité de Microsoft MS05-009 du 08 février 2005:
<http://www.microsoft.com/technet/security/bulletin/MS05-009.msp>
- Référence CVE CAN-2004-0597 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0597>
- Référence CVE CAN-2004-1244 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1244>

Gestion détaillée du document

09 février 2005 version initiale.