

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Winamp

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-2004-AVI-109>

Gestion du document

Référence	CERTA-2004-AVI-109
Titre	Vulnérabilité de Winamp
Date de la première version	06 avril 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité #NISR05042004 de NGSSoftware
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

Versions 5.02 et antérieures.

3 Résumé

Un débordement de mémoire permettant l'exécution de code arbitraire à distance est présent dans Winamp.

4 Description

Le logiciel Winamp permet de lire des fichiers audios et vidéos de différents formats.

Une erreur de type débordement de mémoire est présente dans l'extension permettant de lire les fichiers au format `Fasttracker 2`. Un utilisateur mal intentionné peut, en mettant à disposition des fichiers habilement constitués, exploiter cette faille sur les plate-formes utilisant une version de Winamp vulnérable pour lire ces fichiers malicieux.

5 Contournement provisoire

Il est possible d'invalider l'utilisation de l'extension `Fasttracker 2` en le désélectionnant de la liste des formats supportés (Options->Preferences->Plug-ins->Input->Nullsoft Module Decoder).

6 Solution

La version 5.03 de Winamp corrige cette vulnérabilité :

<http://www.winamp.com/player>

7 Documentation

- Annonce de la disponibilité de la version 5.03 :
http://www.winamp.com/player/version_history.php
- Bulletin de sécurité #NISR05042004 de NGSSoftware :
<http://www.ngssoftware.com/advisories/winampheap.txt>

Gestion détaillée du document

06 avril 2004 version initiale.