

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans 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-378>

Gestion du document

Référence	CERTA-2004-AVI-378-001
Titre	Vulnérabilité dans Winamp
Date de la première version	23 novembre 2004
Date de la dernière version	07 décembre 2004
Source(s)	
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

Winamp version 5.06 et versions antérieures.

3 Résumé

Une vulnérabilité dans un des composants de Winamp permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

4 Description

Winamp est un lecteur multimedia pour Microsoft Windows.

Un débordement de mémoire dans `IN_CDDA.dll` permet à utilisateur mal intentionné, par l'intermédiaire d'un fichier malicieusement constitué et destiné à être lu par Winamp, d'exécuter du code arbitraire à distance sur la plate-forme vulnérable.

La mise à jour 5.06 de Winamp reste vulnérable à cette faille de sécurité.

5 Solution

Mettre à jour Winamp en version 5.07.
Winamp est téléchargeable à l'adresse suivante :
<http://www.winamp.com/player/>

6 Documentation

- Site Internet de Winamp :
<http://www.winamp.com/player/>
- Bulletin de sécurité de security-assessment du 23 novembre 2004 :
http://www.security-assessment.com/Papers/Winamp_IN_CDDA_Buffer_Overflow.pdf

Gestion détaillée du document

23 novembre 2004 version initiale.

07 décembre 2004 Un nouveau correctif permet de corriger cette vulnérabilité.