



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 décembre 2002
N° CERTA-2002-AVI-283

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-2002-AVI-283>

Gestion du document

Référence	CERTA-2002-AVI-283
Titre	Vulnérabilité de Winamp
Date de la première version	27 décembre 2002
Date de la dernière version	–
Source(s)	bulletin d'information de Winamp
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 2.81 et 3.0 (si leur téléchargement a été réalisé avant le 17 décembre 2002).

3 Résumé

Plusieurs débordements de mémoire permettant l'exécution de code arbitraire à distance sont présents dans différentes versions de Winamp.

4 Description

Le logiciel Winamp permet de lire des fichiers au format MP3.

Une mauvaise gestion des balises (*tag*) « ID3v2 artist » par le logiciel Winamp permet d'exécuter du code arbitraire au moyen d'un fichier MP3 habilement construit.

Ces vulnérabilités sont exploitables à distance.

5 Solution

- Pour les utilisateurs de Winamp 2.81 :
Mettre à jour Winamp dans sa dernière version depuis le site web de Winamp :
<http://classic.winamp.com/download>
- Mettre à jour Winamp dans sa dernière version 3.0 *build* #488 depuis le site web de Winamp :
<http://www.winamp.com/download>
Pour vérifier la version de Winamp 3.0 utiliser le menu « A Propos » (ou « *about* »).

6 Documentation

Le bulletin d'information #9680 de Winamp :
<http://www.winamp.com/news.jhtml?articleid=9680>

Gestion détaillée du document

27 décembre 2002 version initiale.