Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 01 septembre 2004
N° CERTA-2004-AVI-287

**Affaire suivie par :**
CERTA

# AVIS DU CERTA

## Objet : Vulnérabilité du logiciel Winamp



## Gestion du document

| | |
|---|---|
| Référence | CERTA-2004-AVI-287 |
| Titre | Vulnérabilité du logiciel Winamp |
| Date de la première version | 01 septembre 2004 |
| Date de la dernière version | – |
| Source(s) | Bulletin de sécurité Winamp du 27 août 2004 |
| 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

- Winamp versions 3.x ;
- Winamp versions 5.04 et antérieures.

## 3 Résumé

Une vulnérabilité du logiciel Winamp permet à un utilisateur mal intentionné d'exécuter du code arbitraire sur le système vulnérable.

## 4 Description

Le logiciel Winamp est un lecteur multimédia pour les plates-formes Windows.

Une vulnérabilité dans la gestion des interfaces (*skin*) par ce lecteur permet à un utilisateur distant d'exécuter du code arbitraire.

Cette vulnérabilité peut être exploitée par le biais d'un site web malicieusement construit qui installe une nouvelle interface sans en informer l'utilisateur. Cette interface peut elle-même faire appel à des pages au format HTML contenant d'éventuels scripts qui seront exécutés dans la zone de sécurité "*Intranet local*".

# 5 Solution

La version 5.05 du logiciel Winamp corrige cette vulnérabilité.

# 6 Documentation

- Site Internet du logiciel Winamp :
  http://www.winamp.com
- Bulletin de sécurité Winamp du 27 août 2004 :
  http://www.winamp.com/about/article.php?aid=10605

# Gestion détaillée du document

**01 septembre 2004** version initiale.