

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-2005-AVI-036>

Gestion du document

| | |
|-----------------------------|---|
| Référence | CERTA-2005-AVI-036 |
| Titre | Vulnérabilité dans WinAMP |
| Date de la première version | 28 janvier 2005 |
| Date de la dernière version | – |
| Source(s) | Message "Buffer Overflow in WinAMP in_cdda.dll CDA Device Name" dans la liste de diffusion Bugtraq du 27 janvier 2005 : |
| Pièce(s) jointe(s) | |

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

Nullsoft WinAMP 5.08 et versions antérieures.

3 Résumé

Une vulnérabilité découverte dans 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.

5 Solution

Mettre à jour Winamp en version 5.08c. Winamp est téléchargeable à l'adresse suivante :
<http://www.winamp.com/player/>

6 Documentation

- Site Internet de Winamp :
<http://www.winamp.com/player/>
- Message "Buffer Overflow in WinAMP in_cdda.dll CDA Device Name" dans la liste de diffusion Bugtraq :
<http://www.securityfocus.com/archive/1/388518/2005-01-31/0>

Gestion détaillée du document

28 janvier 2005 version initiale.