

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités 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-2009-AVI-559>

Gestion du document

Référence	CERTA-2009-AVI-559
Titre	Vulnérabilités dans Winamp
Date de la première version	22 décembre 2009
Date de la dernière version	–
Source(s)	Bulletin de version de Winamp du 21 décembre 2009
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, versions antérieures à la version 5.571.

3 Résumé

Plusieurs vulnérabilités dans Winamp sont exploitables par un utilisateur malveillant pour exécuter du code arbitraire à distance.

4 Description

Plusieurs vulnérabilités sont présentes dans Winamp et permettent à un utilisateur malveillant d'exécuter du code arbitraire à distance en incitant un utilisateur du système vulnérable à ouvrir un fichier spécialement conçu :

- un débordement d'entier survient dans le décodeur *IN_MOD.DLL* lors de l'analyse de certains fichiers de type Oktalyzer, Ultratracker ou Impulse Tracker ;

- plusieurs débordements d’entier sont présents dans les modules *png.w5s* et *jpeg.w5s* et sont exploitables par le biais de fichiers JPEG ou PNG spécifiques contenus dans un fichier MP3.

5 Solution

Migrer en version 5.571.

Se référer au bulletin de sécurité de l’éditeur pour l’obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de version de Winamp du 21 décembre 2009 :
http://www.winamp.com/help/Version_History#Winamp_5.571_.28Latest.29
- Référence CVE CVE-2009-3995 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3995>
- Référence CVE CVE-2009-3996 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3996>
- Référence CVE CVE-2009-3997 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3997>
- Référence CVE CVE-2009-4356 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4356>

Gestion détaillée du document

22 décembre 2009 version initiale.