



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 octobre 2007
N° CERTA-2007-AVI-439

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités de FLAC et 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-2007-AVI-439>

Gestion du document

Référence	CERTA-2007-AVI-439
Titre	Vulnérabilités de FLAC et Winamp
Date de la première version	15 octobre 2007
Date de la dernière version	–
Source(s)	Bulletin iDefense 608 du 11 octobre 2007
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

- *libFLAC* version 1.2.0 ;
- logiciels et distributions incluant cette bibliothèque, dont *Winamp* version 5.35.

3 Résumé

Plusieurs vulnérabilités de la bibliothèque *libFLAC* permettent à un utilisateur malveillant d'exécuter du code arbitraire à distance.

4 Description

FLAC est le sigle du format audio *Free Lossless Audio Codec*.

La bibliothèque *libFLAC* présente des défauts de gestion des fichiers FLAC malformés. Ces défauts provoquent des débordements d'entiers (*integer overflow*). L'exploitation de ces débordements permet à un utilisateur malveillant d'exécuter du code arbitraire à distance.

5 Solution

La version 1.2.1 de la bibliothèque corrige le problème.

La version 5.5 de *Winamp* corrige le problème.

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

6 Documentation

- Bulletin de version de FLAC du 17 septembre 2007 :
<http://flac.sourceforge.net/changelog.html>
- Site de téléchargement de Winamp :
<http://www.winamp.com/player>
- Bulletin de sécurité iDefense du 11 octobre 2007 :
<http://www.iddefense.com/application/poi/display?id=608>
- Référence CVE CVE-2007-4619 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4619>

Gestion détaillée du document

15 octobre 2007 version initiale.