

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités de libsndfile

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-203>

Gestion du document

Référence	CERTA-2009-AVI-203
Titre	Vulnérabilités de libsndfile
Date de la première version	28 mai 2009
Date de la dernière version	–
Source(s)	
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

Bibliothèque libsndfile version 1.0.19 et versions antérieures.

3 Résumé

Plusieurs vulnérabilités de la bibliothèque libsndfile permettent à un utilisateur malveillant d'exécuter à distance du code arbitraire sur le système vulnérable.

4 Description

Plusieurs vulnérabilités de la bibliothèque libsndfile ont été publiées :

- la fonction `header_read()` ne vérifie pas correctement la donnée entrée pour un calcul de taille de tampon en mémoire. Ce défaut peut être utilisé pour provoquer un débordement de zone mémoire ;

- la fonction *aiff_read_header()* ne vérifie pas correctement une borne. Ce défaut peut être utilisé pour provoquer un débordement de zone mémoire ;

Un utilisateur malveillant peut exploiter ces vulnérabilités en incitant un utilisateur à ouvrir un fichier AIFF ou VOC spécialement conçu.

5 Solution

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

6 Documentation

- Bulletin de sécurité Gentoo GLSA-200905-09 du 27 mai 2009 :
<http://www.gentoo.org/security/en/glsa/glsa-200905-09.xml>
- Référence CVE CVE-2009-1788 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1788>
- Référence CVE CVE-2009-1791 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1791>

Gestion détaillée du document

28 mai 2009 version initiale.