

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans FFmpeg

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-2011-AVI-507>

Gestion du document

Référence	CERTA-2011-AVI-507
Titre	Vulnérabilités dans FFmpeg
Date de la première version	13 septembre 2011
Date de la dernière version	–
Source(s)	Buletin de sécurité Debian DSA-2306-1 du 11 septembre 2011
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 ;
- déni de service.

2 Systèmes affectés

Debian Squeeze

3 Résumé

Plusieurs vulnérabilités ont été découverte dans *FFmpeg*.

4 Description

Plusieurs vulnérabilités sont présentes dans *FFmpeg*.

La première (CVE-2010-3908) permet à une personne malintentionnée d'effectuer un déni de service, voire d'exécuter du code arbitraire, lors de l'ouverture d'un fichier WMV spécialement conçu.

La deuxième (CVE-2010-4704) permet de provoquer un déni de service lors de l'ouverture d'un fichier Ogg contrefait.

La troisième (CVE-2011-0480) concerne différents dépassements de tampon dans le décodeur Vorbis, pouvant avoir lieu lors de l'ouverture d'un fichier WebM spécialement formé. Il est alors possible de rendre l'application inopérante (déni de service). Ce problème pourrait avoir d'autres conséquences non déterminées.

La dernière (CVE-2011-0722) permet à un utilisateur malintentionné de provoquer un déni de service ou une exécution de code arbitraire lors de la lecture d'un fichier RealMedia contrefait.

5 Solution

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

6 Documentation

- Bulletin de sécurité Debian DSA 2306 du 11 septembre 2011 :
<http://www.debian.org/security/2011/dsa-2306>
- Référence CVE CVE-2010-3908 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3908>
- Référence CVE CVE-2010-4704 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4704>
- Référence CVE CVE-2011-0480 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0480>
- Référence CVE CVE-2011-0722 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0722>

Gestion détaillée du document

13 septembre 2011 version initiale.