



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 31 janvier 2012
N° CERTA-2012-AVI-039

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-2012-AVI-039>

Gestion du document

Référence	CERTA-2012-AVI-039
Titre	Vulnérabilités dans FFmpeg
Date de la première version	31 janvier 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité FFmpeg
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 ;
- déni de service à distance.

2 Systèmes affectés

FFmpeg versions antérieures à 0.10.

3 Résumé

De multiples vulnérabilités présentes dans FFmpeg permettent d'effectuer une exécution de code ou un déni de service à distance.

4 Description

De multiples vulnérabilités ont été corrigées dans FFmpeg. Ces vulnérabilités permettent à une personne mal-intentionnée d'effectuer une exécution de code ou un déni de service à distance au moyen d'un fichier spécialement conçu.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation). La version 0.10 corrige le problème.

6 Documentation

- Bulletin de sécurité FFmpeg :
<http://ffmpeg.org/security.html>
- Référence CVE CVE-2011-3929 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3929>
- Référence CVE CVE-2011-3934 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3934>
- Référence CVE CVE-2011-3935 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3935>
- Référence CVE CVE-2011-3936 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3936>
- Référence CVE CVE-2011-3937 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3937>
- Référence CVE CVE-2011-3940 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3940>
- Référence CVE CVE-2011-3941 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3941>
- Référence CVE CVE-2011-3944 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3944>
- Référence CVE CVE-2011-3945 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3945>
- Référence CVE CVE-2011-3946 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3946>
- Référence CVE CVE-2011-3947 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3947>
- Référence CVE CVE-2011-3949 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3949>
- Référence CVE CVE-2011-3950 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3950>
- Référence CVE CVE-2011-3951 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3951>
- Référence CVE CVE-2011-3952 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3952>

Gestion détaillée du document

31 janvier 2012 version initiale.