Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 02 avril 2012
N° CERTA-2012-AVI-183

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans libpng

Gestion du document

Référence	CERTA-2012-AVI-183
Titre	Vulnérabilité dans libpng
Date de la première version	02 avril 2012
Date de la dernière version	–
Source(s)	Bulletin de mise à jour libpng du 29 mars 2012
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.

2 Systèmes affectés

- libpng versions 1.5.x antérieures à 1.5.10 ;
- libpng versions 1.4.x antérieures à 1.4.11 ;
- libpng versions 1.2.x antérieures à 1.2.49 ;
- libpng versions 1.0.x antérieures à 1.0.59.

3 Résumé

Une vulnérabilité dans *libpng* permet à une personne malintentionnée de compromettre une application utilisant cette bibliothèque.

4 Description

La vulnérabilité est due à une erreur dans la fonction `png_set_text_2()` et permet à un attaquant de corrompre la mémoire grâce à un fichier PNG spécialement conçu.

L'exploitation de cette vulnérabilité pourrait permettre l'exécution de code arbitraire.

5 Solution

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

6 Documentation

- Référence CVE CVE-2011-3048 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3048
- Bulletin de mise à jour *libpng* 1.5.10 du 29 mars 2012 :
  http://www.libpng.org/pub/png/src/libpng-1.5.10-README.txt
- Bulletin de mise à jour *libpng* 1.2.49 du 29 mars 2012 :
  http://www.libpng.org/pub/png/src/libpng-1.2.49-README.txt

Gestion détaillée du document

02 avril 2012 version initiale.