Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 23 février 2012
N° CERTA-2012-AVI-087-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans libpng

Gestion du document

Référence	CERTA-2012-AVI-087-001
Titre	Vulnérabilité dans libpng
Date de la première version	20 février 2012
Date de la dernière version	23 février 2012
Source	Avertissement sur le site du projet libpng du 19 février 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

Bibliothèque libpng :
- branche 1.0, versions antérieures à la version 1.0.57 ;
- branche 1.2, versions antérieures à la version 1.2.47 ;
- branche 1.4, versions antérieures à la version 1.4.9 ;
- branche 1.5, versions antérieures à la version 1.5.9.

Les applications qui utilisent cette bibliothèque peuvent être vulnérables.

3 Résumé

Une vulnérabilité dans la bibliothèque libpng permet à un attaquant d'exécuter du code arbitraire.

4 Description

Dans la bibliothèque libpng, une erreur d'allocation de mémoire permet à un attaquant, au moyen d'une image au format PNG spécialement construite, d'exécuter du code arbitraire avec les droits de l'utilisateur qui ouvre cette image.

5 Solution

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

6 Documentation

- Avertissement sur le site du projet libpng du 19 février 2012 :
  http://www.libpng.org/pub/png/libpng.html
- Bulletin de sécurité Debian DSA 2410 du 15 février 2012 :
  http://www.debian.org/security/2012/dsa-2410
- Bulletin de sécurité Mandriva MDVSA-2012:022 du 22 février 2012 :
  http://www.mandriva.com/fr/support/security/advisories/?name=MDVSA-2012:022
- Bulletin de sécurité Ubuntu USN-1367-1 du 16 février 2012 :
  http://www.ubuntu.com/usn/usn-1367-1/
- Référence CVE CVE-2011-3026 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3026

Gestion détaillée du document

20 février 2012 version initiale.
23 février 2012 ajout de la référence au bulletin Mandriva.