Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 26 mai 2004
N° CERTA-2004-AVI-148-004

**Affaire suivie par :**
CERTA

# AVIS DU CERTA

## Objet : Vulnérabilité de la bibliothèque libpng



## Gestion du document

| | |
|---|---|
| Référence | CERTA-2004-AVI-148-004 |
| Titre | Vulnérabilité de la bibliothèque libpng |
| Date de la première version | 30 avril 2004 |
| Date de la dernière version | 26 mai 2004 |
| Source(s) | Avis de sécurité Mandrake |
| 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

- Déni de service ;
- exécution de code arbitraire.

## 2 Systèmes affectés

Potentiellement tout système ayant des programmes liés avec la bibliothèque *libpng* versions source 1.2.5 et antérieures.

## 3 Résumé

Une faille dans la gestion des messages d'erreur et d'avertissement peut donner la possibilité à un utilisateur mal intentionné d'exécuter du code arbitraire ou d'entraîner un déni de service sur la machine cible.

## 4 Description

La bibliothèque *libpng* est utilisée par de nombreuses applications (dont les navigateurs, les environnements graphiques KDE et Gnome, certaines distributions LaTeX,. . . ) pour la manipulation de fichiers image au format *png*

(“Portable Network Graphics”). La bibliothèque exporte diverses fonctions, dont deux permettent d’émettre des messages d’erreur ou d’avertissement. Ces fonctions utilisent des tampons de taille fixe, sans vérifier la taille des arguments passés et sans que cette taille maximum soit précisée dans la documentation. Une mauvaise utilisation de ces fonctions dans un programme peut conduire à l’exécution de code arbitraire par débordement de tampon.

# 5 Solution

Mettre à jour en suivant les recommandations des éditeurs :

- Avis de sécurité Mandrake MDKSA-2004:040 :
  http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:040
- Avis de sécurité Debian DSA-498 :
  http://www.debian.org/security/2004/dsa-498
- Avis de sécurité Red Hat Linux
  - Red Hat Desktop, Enterprise et Advanced Workstation RHSA-2004:180 :
    https://rhn.redhat.com/errata/RHSA-2004-180.html
  - Red Hat 9 RHSA-2004:181 :
    https://rhn.redhat.com/errata/RHSA-2004-181.html
- Avis de sécurité Gentoo GLSA 200405-06 du 14 mai 2004 :
  http://www.gentoo.org/security/en/glsa/glsa-200405-06.xml
- Avis de sécurité FreeBSD du 2 mai 2004 :
  http://www.vuxml.org/freebsd/
- Avis de sécurité pour le paquetage OpenBSD libpng du 3 mai 2004 :
  http://www.vuxml.org/openbsd/

# 6 Documentation

Référence CVE CAN-2004-0421 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0421

# Gestion détaillée du document

**30 avril 2004** version initiale.
**03 mai 2004** ajout référence au bulletin de sécurité de Red Hat.
**12 mai 2004** ajout des références aux bulletins de sécurité FreeBSD et OpenBSD.
**17 mai 2004** correction de la référence Mandrake, ajout de la référence au bulletin de sécurité Gentoo.
**26 mai 2004** ajout référence au bulletin de sécurité Red Hat Enterprise.