Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 08 novembre 2007
N° CERTA-2007-AVI-425-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans libpng

Gestion du document

Référence	CERTA-2007-AVI-425-002
Titre	Multiples vulnérabilités dans libpng
Date de la première version	08 octobre 2007
Date de la dernière version	08 novembre 2007
Source(s)	Annonce sur le site officiel du projet libpng
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 à distance.

2 Systèmes affectés

libpng versions 1.2.21 et versions antérieures.

3 Résumé

De multiples vulnérabilités découvertes dans `libpng` permettent à un utilisateur malveillant d'effectuer un déni de service à distance.

4 Description

Plusieurs vulnérabilités affectent la librairie `libpng` :

– une erreur dans la fonction de manipulation de profil peut être exploitée afin de provoquer un dysfonctionnement de l'application utilisant cette bibliothèque ;

- une erreur lors d'une mauvaise utilisation de la fonction *sizeof()* permet d'engendrer un dysfonctionnement de l'application utilisant cette bibliothèque ;
- des erreurs dans les opérations mal contrôlées d'écriture de plusieurs fonctions peuvent être exploitées pour obtenir un dysfontionnement de l'application utilisant cette bibliothèque.

5 Solution

Se référer au bulletin de sécurité sur le site du projet pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Le site officiel du projet libpng :
  http://www.libpng.org/pub/png/libpng.html
- Bulletin de sécurité Gentoo GLSA-200711-08 du 07 novembre 2007 :
  http://www.gentoo.org/security/en/glsa/glsa-200711-08.xml
- Bulletin de sécurité Red Hat RHSA-2007:0992 du 23 octobre 2007 :
  http://rhn.redhat.com/errata/RHSA-2007-0992.html
- Bulletin de sécurité Ubuntu USN-538-1 du 25 octobre 2007 :
  http://www.ubuntu.com/usn/usn-538-1
- Référence CVE CVE-2007-5266 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5266
- Référence CVE CVE-2007-5268 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5268
- Référence CVE CVE-2007-5269 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5269

Gestion détaillée du document

08 octobre 2007 version initiale.
07 novembre 2007 ajout des références CVE et des références aux bulletins de sécurité Ubuntu et Red Hat.
08 novembre 2007 ajout d'une référence CVE et de la référence au bulletin de sécurité Gentoo.