

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans libpng

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-2007-AVI-242>

Gestion du document

| | |
|-----------------------------|---|
| Référence | CERTA-2007-AVI-242 |
| Titre | Vulnérabilité dans libpng |
| Date de la première version | 01 juin 2007 |
| Date de la dernière version | – |
| Source(s) | Bulletin de sécurité Gentoo GLSA-200705-24 du 31 mai 2007 |
| 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 1.x.

3 Résumé

Une vulnérabilité découverte dans la bibliothèque libpng permet à un utilisateur distant malintentionné de provoquer un déni de service à distance.

4 Description

La bibliothèque libpng permet de manipuler les images au format PNG (Portable Network Graphics).

Une vulnérabilité présente dans la fonction `png_handle_trns()` dans le fichier `pngutil.c` permet à un utilisateur distant malintentionné de provoquer un déni de service. Cette vulnérabilité peut être exploitée au moyen d'un fichier image au format png spécialement construit afin de causer l'arrêt brutal de l'application ayant appelé la bibliothèque vulnérable.

5 Solution

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

6 Documentation

- Bulletin de sécurité Gentoo GLSA-200705-24 du 31 mai 2007 :
<http://www.gentoo.org/security/en/glsa/glsa-200705-24.xml>
- Bulletin de sécurité RedHat RHSA-2007:0356 du 17 mai 2007 :
<http://rhn.redhat.com/errata/RHSA-2007-0356.html>
- Référence CVE CVE-2007-2445 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2445>

Gestion détaillée du document

01 juin 2007 version initiale.