

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans la bibliothèque 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-2006-AVI-059>

Gestion du document

Référence	CERTA-2006-AVI-059-001
Titre	Vulnérabilité dans la bibliothèque libpng
Date de la première version	08 février 2006
Date de la dernière version	08 mars 2006
Source(s)	Annonce de mise à jour de sécurité sur le site de 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

- Exécution de code arbitraire à distance ;
- déni de service à distance.

2 Systèmes affectés

- libpng versions 1.0.17 et antérieures ;
- libpng versions 1.2.7 et antérieures.

3 Résumé

Une vulnérabilité dans la bibliothèque de fonctions libpng permet à un utilisateur distant mal intentionné de réaliser un déni de service ou potentiellement d'exécuter du code arbitraire.

4 Description

Une erreur dans la fonction `png_set_strip_alpha()` de la bibliothèque de fonctions libpng permet à un utilisateur distant mal intentionné de réaliser un débordement de mémoire par le biais d'une image de type PNG

(Portable Network Graphics) malicieusement construite. Il peut ainsi réaliser un déni de service sur l'application utilisant cette fonction ou potentiellement exécuter du code arbitraire.

5 Solution

Les versions 1.0.18 et 1.2.8 corrigent le problème :

<http://www.libpng.org/pub/png/libpng.html>

6 Documentation

- Site Internet de libpng :
<http://www.libpng.org/pub/png/libpng.html>
- Bulletin de sécurité RedHat RHSA-2006:0205 du 13 février 2006 :
<https://rhn.redhat.com/errata/RHSA-2006-0205.html>
- Référence CVE CAN-2006-0481 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-0481>

Gestion détaillée du document

08 février 2006 version initiale.

08 mars 2006 ajout de la référence au bulletin de sécurité RedHat.