

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-2003-AVI-003>

---

### Gestion du document

Référence	CERTA-2003-AVI-003-001
Titre	Vulnérabilité dans la bibliothèque libpng
Date de la première version	14 janvier 2003
Date de la dernière version	21 janvier 2003
Source(s)	Bulletin de sécurité DSA-213 de Debian Bulletin de sécurité SuSE-SA:2003:0004 de SuSE Bulletin de sécurité RHSA-2003:006 de Red Hat
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 à distance.

## 2 Systèmes affectés

Tous système ayant une bibliothèque libpng version 1.2.1 ou antérieure.

## 3 Résumé

Une vulnérabilité présente dans la bibliothèque libpng permet 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) pour la manipulation de fichiers image au format `png` (Portable Neutral Graphics).

Une vulnérabilité de type débordement de mémoire présente dans la bibliothèque `libpng` permet à un utilisateur mal intentionné d'exécuter du code arbitraire ou d'entraîner un déni de service sur la machine cible au moyen d'un fichier judicieusement composé.

## 5 Solution

Se référer aux bulletins de sécurité des différents éditeurs pour connaître la disponibilité des correctifs (cf. section Documentation).

## 6 Documentation

- Bulletin de sécurité RHSA-2003:006 de Red Hat :  
<http://rhn.redhat.com/errata/RHSA-2003-006.html>
- Bulletin de sécurité DSA-213 de Debian :  
<http://www.debian.org/security/2002/dsa-213>
- Bulletin de sécurité SuSE-SA:2003:0004 de SuSE :  
[http://www.suse.com/de/security/2003\\_004\\_libpng.html](http://www.suse.com/de/security/2003_004_libpng.html)
- Bulletin de sécurité MDKSA-2003:008 de Mandrake :  
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:008>

## Gestion détaillée du document

**14 janvier 2003** version initiale.

**21 janvier 2003** ajout référence au bulletin de sécurité MDKSA-2003:008 de Mandrake.