Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 août 2002
N° CERTA-2002-AVI-166-003

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans la bibliothèque libpng

Gestion du document

Référence	CERTA-2002-AVI-166-003
Titre	Vulnérabilité dans la bibliotheque libpng
Date de la première version	02 août 2002
Date de la dernière version	20 août 2002
Source(s)	Bulletin de sécurité DEBIAN
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 ;
- déni de service.

2 Systèmes affectés

Tout système ayant la bibliothèque `libpng2` ou `libpng3` installée.

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 nombreuse applications (dont les navigateurs) pour la manipulation de fichiers image au format `png`.

Un débordement de mémoire dans la gestion de la taille des données (la taille des données spécifiée dans la section IHDR est inférieure à la taille des données effectivement reçues) permet à un utilisateur mal intentionné, composant judicieusement un fichier destiné à être lu par cette bibliothèque, d'exécuter du code arbitraire ou d'entraîner un déni de service de l'application sur la machine cible.

5 Solution

Les versions 1.0.14 et 1.2.14 de la bibliothèque corrigent cette vulnérabilité.
Consulter les bulletins de sécurité de votre distributeur pour connaître la disponibilité des correctifs.

6 Documentation

- Avis de sécurité DSA 140-1 et DSA 140-2 de Debian :
  http://www.debian.org/security
- Avis de sécurité MDKSA-2002:049 de Mandrake :
  http://www.mandrakesecure.net/en/advisories/2002/MDKSA-2002-049.php
- Avis de sécurité RHSA-2002:151 de Red Hat :
  http://rhn.redhat.com/errata/RHSA-2002-151.html

Gestion détaillée du document

02 août 2002 version initiale.

06 août 2002 ajout de l'avis de sécurité DSA 140-2 concernant un débordement de mémoire supplémentaire.

19 août 2002 ajout de la référence à l'avis de sécurité MDKSA-2002:049 de Mandrake.

20 août 2002 modification de la section Description, mention des versions non vulnérables, ajout de la référence à l'avis de sécurité RHSA-2002:151 de Red Hat.