Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 octobre 2004
N° CERTA-2004-AVI-353

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples Vulérabilités dans les bibliothèques libpng

Gestion du document

Référence	CERTA-2004-AVI-353
Titre	Multiples vulérabilités dans les bibliothèques libpng
Date de la première version	21 octobre 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité Debian DSA-570 du 20 octobre 2004 Bulletin de sécurité Debian DSA-571 du 20 octobre 2004
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

Execution de code arbitraire.

2 Systèmes affectés

- Bibliothèque libpng 1.0.12-3 et versions antérieures ;
- bibliothèque libpng 1.0.15-8 et versions antérieures ;
- bibliothèque libpng3 1.2.1-1.1 et versions antérieures ;
- bibliothèque libpng3 1.2.5.0-9 et versions antérieures.

3 Résumé

Les vulnérabilités découvertes dans les bibliothèques `libpng` et `libpng3` permettent à un utilisateur mal intentionné d'exécuter du code arbitraire sur le système vulnérable.

4 Description

Les bibliothèques `libpng` et `libpng3` sont utilisées par de nombreuses applications pour la manipulation de fichier au format `png` ("`Portable Network Graphics`"). Plusieurs vulnérabilités ont été découvertes dans ces bibliothèques :

- Ces deux bibliothèques présentent des vulnérabilités de type débordement d'entier (`integer overflow`). Un utilisateur mal intentionné peut ainsi exécuter un code arbitraire sur le système vulnérable au moyen d'une image au format `png` malicieusement constituée.
- De plus, la bibliothèque `libpng3` présente une vulnérabilité de type débordement de mémoire.

5 Solution

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

6 Documentation

- Bulletin de sécurité Debian DSA-570 du 20 octobre 2004 :
  http://debian.org/security/2004/dsa-570
- Bulletin de sécurité Debian DSA-571 du 20 octobre 2004 :
  http://debian.org/security/2004/dsa-571
- Référence CVE CAN-2004-0955 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0955

Gestion détaillée du document

21 octobre 2004 version initiale.