Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 juin 2009
N° CERTA-2009-AVI-073-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans libpng

Gestion du document

Référence	CERTA-2009-AVI-073-002
Titre	Vulnérabilité dans libpng
Date de la première version	20 février 2009
Date de la dernière version	12 juin 2009
Source(s)	Bulletin de sécurité du projet 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.

2 Systèmes affectés

- Toutes les versions antérieures à la 1.0.43 ;
- toutes les versions antérieures à la 1.2.35.

3 Résumé

Une vulnérabilité dans `libpng` permet à une personne malintentionnée d'exécuter du code arbitraire à distance.

4 Description

Une erreur dans la gestion des tableaux de pointeur de `libpng` permet à une personne malveillante d'exécuter du code arbitraire à distance via un fichier *PNG* spécialement construit.

5 Solution

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

6 Documentation

- Site de téléchargement du projet libpng :
  http://sourceforge.net/projects/libpng
- Bulletin de sécurité du projet libpng :
  http://downloads.sourceforge.net/libpng/libpng-1.2.34-ADVISORY.txt
- Bulletin de sécurité Gentoo GLSA-200804-15 du 15 avril 2008 :
  http://www.gentoo.org/security/en/glsa/glsa-200804-15.xml
- Bulletin de sécurité Red Hat RHSA-2009:0333 du 04 mars 2009 :
  http://rhn.redhat.com/errata/RHSA-2009-0333.html
- Bulletin de sécurité Red Hat RHSA-2009:0340 du 04 mars 2009 :
  http://rhn.redhat.com/errata/RHSA-2009-0340.html
- Bulletin de sécurité SuSE SuSE-SR:2009:005 du 02 mars 2009 :
  http://lists.opensuse.org/opensuse-security-announce/2009-03/msg00000.html
- Bulletin de sécurité VMware VMSA-2009-0007 :
  http://www.vmware.com/security/advisories/VMSA-2009-0007.html
- Bulletin de sécurité Sun Solaris du 28 mai 2009 :
  http://sunsolve.sun.com/search/document.do?assetkey=1-66-259989-1
- Référence CVE CVE-2009-0040 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0040

Gestion détaillée du document

20 février 2009 version initiale.
06 mars 2009 ajout des références aux bulletins de sécurité Gentoo, Red Hat et SuSE.
12 juin 2009 ajout des références aux bulletins de sécurité VMware et Sun Solaris.