



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 06 décembre 2004
N° CERTA-2004-AVI-266-005

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de 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-2004-AVI-266>

Gestion du document

Référence	CERTA-2004-AVI-266-005
Titre	Multiples vulnérabilités de la bibliothèque libpng
Date de la première version	05 août 2004
Date de la dernière version	06 décembre 2004
Source(s)	Avis de sécurité de Chris Evans
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

- Bibliothèque *libpng* versions 1.2.5 et antérieures ;
- bibliothèque *libpng* versions 1.0.15 et antérieures.

3 Résumé

Plusieurs vulnérabilités de la bibliothèque *libpng* permettent à un utilisateur distant mal intentionné d'exécuter du code arbitraire sur le système vulnérable ou de provoquer un déni de service.

4 Description

La bibliothèque *libpng* est utilisée par de nombreuses applications (dont les navigateurs, les environnements graphiques KDE et Gnome, certaines distributions \LaTeX ,...) pour la manipulation de fichiers image au format *png* ("Portable Network Graphics").

Plusieurs vulnérabilités ont été découvertes dans cette bibliothèque :

- CVE CAN-2004-0597 : plusieurs failles de type débordement de mémoire permettent d'exécuter du code arbitraire via un fichier au format png habilement construit ;
- CVE CAN-2004-0598 : une vulnérabilité de la fonction *png_handle_iCCP* permet à un utilisateur distant de provoquer un déni de service ;
- CVE CAN-2004-0599 : plusieurs vulnérabilités de type débordement d'entier (*integer overflow*) ont été découvertes dans les fonctions *png_read_png* et *png_handle_sPLT* et dans la gestion de l'affichage de certaines images png.

5 Solution

Les versions 1.2.6rc1 et 1.0.16rc1 de la bibliothèque *libpng* corrigent ces vulnérabilités.

6 Documentation

- Site Internet de la bibliothèque *libpng* :
<http://www.libpng.org/pub/png/libpng.html>
- Avis de sécurité de Chris Evans 2004.1 :
<http://scary.beasts.org/security/CESA-2004-001.txt>
- Alerte de sécurité de l'US-CERT TA04-217A du 04 août 2004 :
<http://www.us-cert.gov/cas/techalerts/TA04-217A.html>
- Bulletin de sécurité Debian DSA-536 du 04 août 2004 :
<http://www.debian.org/security/2004/dsa-536>
- Bulletin de sécurité Gentoo GLSA-200408-03 du 05 août 2004 :
<http://www.gentoo.org/security/en/glsa/glsa-200408-03.xml>
- Bulletin de sécurité Mandrake MDKSA-2004:079 du 04 août 2004 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:079>
- Bulletin de sécurité RedHat RHSA-2004:402 du 04 août 2004 :
<http://rhn.redhat.com/errata/RHSA-2004-402.html>
- Bulletin de sécurité SUSE SuSE-SA:2004:023 du 04 août 2004 :
http://www.suse.com/de/security/2004_23_libpng.html
- Bulletin de sécurité FreeBSD pour libPNG du 04 août 2004 :
<http://www.vuxml.org/freebsd/>
- Bulletin de sécurité OpenBSD pour libPNG du 04 août 2004 :
<http://www.vuxml.org/openbsd>
- Bulletin de sécurité de Mozilla - Bug #251381 :
http://bugzilla.mozilla.org/show_bug.cgi?id=251381
- Bulletin de sécurité HP pour Mozilla HPSBTU01063 du 04 août 2004 :
<http://www5.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBTU01063>
- Bulletin de sécurité de Sun #57617 du 06 août 2004 :
<http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/57617>
- Bulletin de sécurité de Sun #57683 du 30 novembre 2004 :
<http://sunsolve.sun.com/search/document.dp?assetkey=1-26-57683-1>
- Bulletin de sécurité Apple du 09 août 2004 :
<http://www.info.apple.com/kbnum/n61798>
- Référence CVE CAN-2004-0597 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0597>
- Référence CVE CAN-2004-0598 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0598>
- Référence CVE CAN-2004-0599 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0599>

Gestion détaillée du document

05 août 2004 version initiale.

06 août 2004 ajout des références aux bulletins de sécurité Debian, Mandrake et Mozilla.

06 août 2004 ajout des références aux bulletins de sécurité FreeBSD et OpenBSD.

07 août 2004 ajout de la référence au bulletin de sécurité HP.

10 août 2004 ajout des références aux bulletins de sécurité Sun et Apple.

06 décembre 2004 ajout de la référence au bulletin de sécurité Sun #57683 relatif à Netscape.