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-345-005

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de Libtiff

Gestion du document

Référence	CERTA-2004-AVI-345-005
Titre	Multiples vulnérabilités de Libtiff
Date de la première version	15 octobre 2004
Date de la dernière version	06 decembre 2004
Source(s)	Bulletin de sécurité GLSA 200410-11 de Gentoo
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 ;
- déni de service.

2 Systèmes affectés

Libtiff v3.6.1 et versions antérieures.
Le paquetage wxGTK2 et la bibliothèque PDFlib réutilisant du code de libtiff sont également vulnérables.

3 Description

Le paquetage `Libtiff` comprend une bibliothèque et un ensemble d'outils pour le traitement des images au format TIFF (Tag Image File Format).

De multiples vulnérabilités de type débordement de mémoire sont présentes dans la bibliothèque `Libtiff`.
Ces vulnérabilités peuvent être exploitées par un utilisateur mal intentionné afin de réaliser un déni de service ou exécuter du code arbitraire sur le système vulnérable.

4 Solution

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

5 Documentation

- Site de Libtiff :
  http://www.libtiff.org
- Bulletin de sécurité de Chris Evans :
  http://scary.beasts.org/security/CESA-2004-006.txt
- Bulletin de sécurité Gentoo GLSA 200410-11 du 13 octobre 2004 :
  http://www.gentoo.org/security/en/glsa/glsa-200410-11.xml
- Bulletin de sécurité Debian DSA-567 du 15 octobre 2004 :
  http://www.debian.org/security/2004/dsa-567
- Bulletin de sécurité Mandrake MDKSA-2004:109 du 19 octobre 2004 :
  http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:109
- Bulletin de sécurité Mandrake MDKSA-2004:111 du 21 octobre 2004 :
  http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:111
- Bulletin de sécurité FreeBSD "Tiff – multiple integer overflows" du 13 octobre 2004 :
  http://www.vuxml.org/freebsd
- Bulletin de sécurité FreeBSD "Tiff – RLE decoder heap overflows" du 13 octobre 2004 :
  http://www.vuxml.org/freebsd
- Bulletin de sécurité Red Hat RHSA-2004:577 du 22 octobre 2004 :
  http://rhn.redhat.com/errata/RHSA-2004-577.html
- Bulletin de sécurité d'iDEFENSE "Novell SuSE Linux libTIFF heap overflow vulnerability" du 22 octobre 2004 :
  http://www.idefense.com/application/poi/display?id=154&type=vulnerabilities
- Bulletin de sécurité SuSE SuSE-SA:2004:038 du 22 octobre 2004 :
  http://www.suse.de/de/security/2004_38_libtiff.html
- Annonce de PDFlib 5.0.4p1 le 15 novembre 2004 :
  http://www.pdflib.com/products/pdflib/info/PDFlib-5.0.4p1-changes.txt
- Bulletin de sécurité Gentoo GLSA 200412-02 du 05 decembre 2004 :
  http://www.gentoo.org/security/en/glsa/glsa-200412-02.xml
- Bulletin de sécurité d'Apple du 02 décembre 2004 :
  http://docs.info.apple.com/article.html?artnum=61798
- Référence CVE CAN-2004-0803 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0803
- Référence CVE CAN-2004-0804 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0804
- Référence CVE CAN-2004-0886 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0886
- Référence CVE CAN-2004-0929 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0929

Gestion détaillée du document

15 octobre 2004 version initiale.

18 octobre 2004 ajout référence au bulletin de sécurité DSA-567 de Debian. Ajout référence CVE CAN-2004-0804.

20 octobre 2004 ajout référence au bulletin de sécurité MDKSA-2004:109 de Mandrake.

22 octobre 2004 ajout référence au bulletin de sécurité MDKSA-2004:111 de Mandrake relatif à wxGTK2.

25 octobre 2004 ajout référence au bulletin de sécurité de Red Hat. Ajout référence à la vulnérabilité CAN-2004-0929 ainsi qu'aux documents associés (bulletin SUSE-SA:2004:038 et bulletin d'iDEFENSE).

06 décembre 2004 ajout référence au bulletin de sécurité d'Apple. Ajout référence à la PDFlib ainsi qu'au bulletin GLSA-200412-02.