Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 03 juin 2005
N° CERTA-2005-AVI-003-007

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de libtiff

Gestion du document

Référence	CERTA-2005-AVI-003-007
Titre	Multiples vulnérabilités de libtiff
Date de la première version	04 janvier 2005
Date de la dernière version	03 juin 2005
Source(s)	Bulletin de sécurité DSA-617 de 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 à distance ;
- déni de service.

2 Systèmes affectés

Libtiff v3.7.0 et versions antérieures.

3 Description

Libtiff est une bibliothèque 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.
En incitant un utilisateur à visualiser une image au format TIFF habilement constituée, ces vulnérabilités peuvent être exploitées afin d'exécuter du code arbitraire via une application utilisant la bibliothèque vulnérable.

4 Solution

La version 3.7.1 de la bibliothèque libtiff corrige cette vulnérabilité.
Se référer aux bulletins de sécurité de l'éditeur (cf. section Documentation) pour l'obtention des correctifs.

5 Documentation

- Source de libtiff :
  ftp://ftp.remotesensing.org/pub/libtiff/
- Bulletin de sécurité #174 d'iDEFENSE du 21 décembre 2004 :
  http://www.idefense.com/application/poi/display?id=174&type=vulnerabilities
- Bulletin de sécurité Debian DSA-617 du 24 décembre 2004 :
  http://www.debian.org/security/2004/dsa-617
- Bulletin de sécurité Debian DSA-626 du 06 janvier 2005 :
  http://www.debian.org/security/2004/dsa-626
- Bulletin de sécurité Gentoo GLSA 200501-06 du 05 janvier 2005 :
  http://www.gentoo.org/security/en/glsa/glsa-200501-06.xml
- Bulletin de sécurité Mandrake MDKSA-2005:001 du 6 janvier 2005 :
  http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:001
- Bulletin de sécurité Mandrake MDKSA-2005:052 du 04 mars 2005 :
  http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:052
- Bulletin de sécurité SUSE SuSE-SA:2005:001 du 10 janvier 2005 :
  http://www.novell.com/linux/security/advisories/2005_01_libtiff_tiff.html
- Bulletin de sécurité RedHat RHSA-2005:019 du 13 janvier 2005 :
  http://rhn.redhat.com/errata/RHSA-2005-019.html
- Bulletin de sécurité RedHat RHSA-2005:035 du 15 janvier 2005 :
  http://rhn.redhat.com/errata/RHSA-2005-035.html
- Bulletins de sécurité FreeBSD du 06 janvier 2005 relatifs à tiff :
  http://www.vuxml/freebsd/
- Bulletin de sécurité Sun #57769 du 27 avril 2005 :
  http://sunsolve.sun.com/search/document.do?assetkey=1-26-57769-1
- Référence CVE CAN-2004-1308 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1308
- Référence CVE CAN-2004-1183 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1183

Gestion détaillée du document

04 janvier 2005 version initiale.

06 janvier 2005 ajout référence au bulletin de sécurité Gentoo GLSA 200501-06. Ajout référence CVE 1308.

07 janvier 2005 ajout références aux bulletins de sécurité Mandrake MDKSA-2005:001, Debian DSA-626 et bulletins FreeBSD. Ajout référence CVE 1183.

12 janvier 2005 ajout référence au bulletin de sécurité SUSE SuSE-SA:2005:001.

14 janvier 2005 ajout référence au bulletin de sécurité RedHat RHSA-2005:019.

17 février 2005 ajout référence au bulletin de sécurité RedHat RHSA-2005:035.

08 mars 2005 ajout référence au bulletin de sécurité Mandrake MDKSA-2005:052.

03 juin 2005 ajout référence au bulletin de sécurité #57769 de Sun.