



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 01 juin 2006
N° CERTA-2006-AVI-224

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples Vulnérabilités dans libTIFF

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-2006-AVI-224>

Gestion du document

Référence	CERTA-2006-AVI-224
Titre	Multiples Vulnérabilités dans libTIFF
Date de la première version	01 juin 2006
Date de la dernière version	-
Source(s)	Liste des changements apportés dans la version 3.8.1 de libTIFF
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 à distance.

2 Systèmes affectés

libTIFF versions 3.8.0 et antérieures.

3 Résumé

De multiples vulnérabilités dans la bibliothèque de fonctions libTIFF permettent à un utilisateur distant mal intentionné de provoquer un déni de service ou d'exécuter du code arbitraire.

4 Description

La bibliothèque de fonctions libTIFF est utilisée pour l'affichage ou la manipulation d'images au format TIFF dans diverses applications comme l'éditeur d'images The GIMP.

Trois vulnérabilités sont présentes dans la `libTIFF` :

- Une erreur non spécifiée dans la fonction `TIFFFetchAnyArray()` permet de provoquer un déni de service de l'application utilisant cette fonction ;
- une erreur dans la fonction `TIFFFetchData()` permet de provoquer un déni de service de l'application utilisant cette fonction ou d'exécuter du code arbitraire à distance ;
- une erreur dans le fichier `tif_jpeg.c` permet à un utilisateur distant mal intentionné de provoquer un déni de service de l'application utilisant une fonction vulnérable de ce fichier ou d'exécuter du code arbitraire.

Toutes ces vulnérabilités sont exploitables par le biais d'une image particulière au format TIFF.

5 Solution

La version 3.8.1 corrige ces problèmes :

<http://www.remotesensing.org/libtiff/>

6 Documentation

- Liste des changements apportés à la version 3.8.1 de `libTIFF` :
<http://www.remotesensing.org/libtiff/3.8.1.html>
- Bulletin de sécurité Debian DSA 1054 du 27 mai 2006 :
<http://www.debian.org/security/dsa-1054>
- Bulletin de sécurité Debian DSA 1078 du 27 mai 2006 :
<http://www.debian.org/security/dsa-1078>
- Bulletin de sécurité Gentoo GLSA-200605-17 du 31 mai 2006 :
<http://www.gentoo.org/security/en/glsa/glsa-200605-17.xml>
- Référence CVE CVE-2006-0405 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0405>
- Référence CVE CVE-2006-2024 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2024>
- Référence CVE CVE-2006-2025 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2025>
- Référence CVE CVE-2006-2026 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2026>

Gestion détaillée du document

01 juin 2006 version initiale.