



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 29 juin 2010
N° CERTA-2010-AVI-281-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : 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-2010-AVI-281>

Gestion du document

Référence	CERTA-2010-AVI-281-001
Titre	Vulnérabilités dans LibTIFF
Date de la première version	23 juin 2010
Date de la dernière version	29 juin 2010
Source(s)	Bulletin de la version 3.9.4 de la bibliothèque LibTIFF du 15 juin 2010
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.

2 Systèmes affectés

LibTIFF version 3.9.3 et versions antérieures.
Les applications utilisant cette bibliothèque peuvent être vulnérables.

3 Résumé

Deux vulnérabilités dans le traitement d'images par LibTIFF sont exploitables par un utilisateur malveillant pour exécuter du code arbitraire.

4 Description

Un débordement de mémoire peut survenir lors du traitement du champ *SubjectDistance* dans une image au format TIFF. Cette vulnérabilité est exploitable par un utilisateur malveillant pour exécuter du code arbitraire au moyen d'une image TIFF spécialement conçue (CVE-2010-2067).

La correction de la vulnérabilité référencée CVE-2010-2347, permettant de l'exécution de code arbitraire, était incomplète.

5 Solution

La version 3.9.4 de la bibliothèque LibTIFF remédie à ce problème.
Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de la version 3.9.4 de la bibliothèque LibTIFF du 15 juin 2010 :
<http://www.remotesensing.org/libtiff/v3.9.4.html>
- Référence CVE CVE-2010-2067 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2067>
- Référence CVE CVE-2010-2347 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2347>

Gestion détaillée du document

23 juin 2010 version initiale.

29 juin 2010 précision sur une seconde vulnérabilité.