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-262-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans LibTIFF

Gestion du document

Référence	CERTA-2010-AVI-262-001
Titre	Vulnérabilités dans LibTIFF
Date de la première version	14 juin 2010
Date de la dernière version	29 juin 2010
Source(s)	Bulletin de la version 3.9.3 de la bibliothèque LibTIFF du 11 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 3.9.2 et versions antérieures.
Les applications utilisant cette bibliothèque peuvent être vulnérables.

3 Résumé

Des vulnérabilités dans des décodeurs de la bibliothèque LibTIFF sont exploitables par un utilisateur malveillant pour exécuter du code arbitraire.

4 Description

Un débordement d'entier affecte le décodeur d'une catégorie d'images au format TIFF (FAX3). Cette vulnérabilité est exploitable par un utilisateur malveillant pour exécuter du code arbitraire.

Un autre débordement d'entier, dans le traitement d'une macro, permet à un utilisateur malveillant de provoquer un déni de service et, potentiellement, d'exécuter du code arbitraire.

Un problème de traitement du format OJPEG est exploitable par un utilisateur malveillant pour provoquer un déni de service.

5 Solution

La version 3.9.3 de la bibliothèque LibTIFF remédie à ces problèmes.
À la date de mise à jour de cet avis, des vulnérabilités de la version 3.9.3 sont corrigées par la version 3.9.4.
Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de la version 3.9.3 de la bibliothèque LibTIFF du 11 juin 2010 :
  http://www.remotesensing.org/libtiff/v3.9.3.html
- Référence CVE CVE-2010-1411 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1411
- Référence CVE CVE-2010-2065 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2065
- Référence CVE CVE-2010-2443 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2443

Gestion détaillée du document

14 juin 2010 version initiale.
29 juin 2010 ajout d'autres vulnérabilités et des références CVE correspondantes.