

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans la bibliothèque 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-2009-AVI-284>

Gestion du document

Référence	CERTA-2009-AVI-284
Titre	Vulnérabilités dans la bibliothèque libtiff
Date de la première version	21 juillet 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Debian DSA-1835 du 15 juillet 2009
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 3.x.

3 Résumé

Deux vulnérabilités découvertes dans la bibliothèque LibTIFF permettent à un utilisateur distant malintentionné de provoquer un déni de service ou d'exécuter du code arbitraire.

4 Description

Deux vulnérabilités de type débordement de mémoire ont été découvertes dans les fonctions `LZWDecodeCompat()`, `tiffcvt()` et `cvt_whole_image()`. Ces vulnérabilités peuvent être exploitées à distance afin de provoquer un déni de service ou d'exécuter du code arbitraire au moyen d'un fichier au format TIFF spécialement construit.

5 Solution

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

6 Documentation

- Bulletin de sécurité Debian DSA 1835 du 15 juillet 2009 :
<http://www.debian.org/security/2009/dsa-1835>
- Bulletin de sécurité RedHat RHSA-2009:1159 du 16 juillet 2009 :
<http://rhn.redhat.com/errata/RHSA-2009-1159.html>
- Bulletin de sécurité Ubuntu USN-797-1 du 06 juillet 2009 :
<http://www.ubuntulinux.org/usn/usn-797-1>
- Bulletin de sécurité Ubuntu USN-801-1 du 13 juillet 2009 :
<http://www.ubuntulinux.org/usn/usn-801-1>
- Référence CVE CVE-2009-2285 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2285>
- Référence CVE CVE-2009-2347 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2347>

Gestion détaillée du document

21 juillet 2009 version initiale.