

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans la bibliothèque imlib2

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-488>

Gestion du document

Référence	CERTA-2006-AVI-488-001
Titre	Vulnérabilités dans la bibliothèque imlib2
Date de la première version	09 novembre 2006
Date de la dernière version	21 décembre 2006
Source(s)	CVE-2006-4806 CVE-2006-4807 CVE-2006-4808 CVE-2006-4809
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 ;
- déni de service.

2 Systèmes affectés

Les versions de la bibliothèque de fonctions `Imlib2` compilées à partir de sources antérieures à la version 1.2.0-2.2.

3 Description

`Imlib2` est une bibliothèque de fonctions destinées à manipuler et afficher des images dans différents formats. Certaines applications dépendent de cette bibliothèque de fonction.

Des vulnérabilités affectent cette bibliothèque de fonctions. Elles peuvent être exploitées pour commettre un déni de service et potentiellement compromettre le système au travers des applications qui utilisent cette bibliothèque.

Les vulnérabilités sont dues à des erreurs dans le traitement d'images au format JPG, ARGB, PNG, LBM, PNM, TIFF et TGA.

L'exploitation peut être obtenue par un individu mal intentionné qui serait à même de convaincre une victime d'ouvrir une image astucieusement construite avec une application s'appuyant sur une version vulnérable de la bibliothèque.

4 Solution

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

5 Documentation

- Bulletin de sécurité Mandriva MDKSA-2006:198 du 06 novembre 2006 :
<http://www.new.mandriva.com/security/advisories?name=MDKSA-2006:198>
- Bulletin de sécurité Ubuntu USN-376-1 du 03 novembre 2006 :
<http://www.ubuntulinux.org/usn/usn-376-1>
- Bulletin de sécurité Ubuntu USN-376-2 du 03 novembre 2006 :
<http://www.ubuntulinux.org/usn/usn-376-2>
- Bulletin de sécurité Gentoo GLSA-200612-20 du 20 décembre 2006 :
<http://www.gentoo.org/security/en/glsa/glsa-200612-20.xml>
- Bulletin de sécurité SuSE SUSE-SR:2006:026 du 17 novembre 2006 :
<http://lists.suse.com/archive/suse-security-announce/2006-Nov/0008.html>
- Référence CVE CVE-2006-4806 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4806>
- Référence CVE CVE-2006-4807 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4807>
- Référence CVE CVE-2006-4808 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4808>
- Référence CVE CVE-2006-4809 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4809>

Gestion détaillée du document

09 novembre 2006 version initiale.

21 décembre 2006 ajout de la référence au bulletin de sécurité Gentoo.