

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de libexif

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-2005-AVI-105>

Gestion du document

| | |
|-----------------------------|--|
| Référence | CERTA-2005-AVI-105-005 |
| Titre | Vulnérabilité de libexif |
| Date de la première version | 11 mars 2005 |
| Date de la dernière version | 24 novembre 2005 |
| Source(s) | Bulletin de sécurité FreeBSD du 08 mars 2005 |
| Pièce(s) jointe(s) | |

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

- Déni de service ;
- accès au système.

2 Systèmes affectés

Toutes les versions antérieures à libexif 0.6.10_1.

3 Description

La bibliothèque libexif est utilisée pour interpréter les fichiers image au format EXIF.

Une vulnérabilité de type débordement de mémoire permet à un utilisateur mal intentionné d'avoir un accès au système vulnérable ou d'effectuer un déni de service à distance sur n'importe quelle application utilisant la bibliothèque libexif,

4 Solution

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

5 Documentation

- Bulletin de sécurité Mandrake MDKSA-2005:064 du 31 mars 2005 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:064>
- Mise à jour de sécurité pour Fedora Core 2 du 8 mars 2005 :
<http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/>
- Mise à jour de sécurité pour Fedora Core 3 du 8 mars 2005 :
<http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/>
- Bulletin de sécurité FreeBSD du 08 mars 2005 pour libexif :
<http://www.vuxml.org/freebsd/pkg-libexif.html>
- Bulletin de sécurité OpenBSD du 13 mars 2005 pour libexif :
<http://www.vuxml.org/openbsd>
- Bulletin de sécurité Gentoo GLSA 200503-17 du 12 mars 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200503-17.xml>
- Bulletin de sécurité Red Hat RHSA-2005:300 du 21 mars 2005 :
<https://rhn.redhat.com/errata/RHSA-2005-300.html>
- Bulletin de sécurité Debian DSA-709 du 15 avril 2005 :
<http://www.debian.org/security/2005/dsa-709>
- Bulletin de sécurité de Sun #102041 du 23 novembre 2005 :
<http://sunsolve.sun.com/searchproxy/document.do?assetkey=1-26-102041-1>
- Référence CVE CAN-2005-0664 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0664>

Gestion détaillée du document

11 mars 2005 version initiale.

17 mars 2005 ajout référence au bulletin de sécurité de Gentoo.

24 mars 2005 ajout référence au bulletin de sécurité OpenBSD et RedHat RHSA-2005:300.

01 avril 2005 ajout référence au bulletin de sécurité Mandrake.

18 avril 2005 ajout référence au bulletin de sécurité Debian.

24 novembre 2005 ajout référence au bulletin de sécurité Sun #102041.