

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans 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-2012-AVI-392>

---

### Gestion du document

Référence	CERTA-2012-AVI-392
Titre	Vulnérabilité dans libexif
Date de la première version	17 juillet 2012
Date de la dernière version	-
Source(s)	Notes de modifications de la version 0.6.21 de libexif du 12 juillet 2012
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

libexif versions 0.6.20 et antérieures.

## 3 Résumé

Plusieurs vulnérabilités ont été corrigées dans *libexif*. Plusieurs d'entre elles concernent des débordement de tampon. Elles permettent à un utilisateur malintentionné d'exécuter du code arbitraire au moyen d'une image contenant des tags EXIF spécialement conçus.

## 4 Solution

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

## 5 Documentation

- Notes de modifications de la version 0.6.21 de libexif du 12 juillet 2012 :  
[http://libexif.cvs.sourceforge.net/viewvc/libexif/libexif/NEWS?view=markup&pathrev=libexif-0\\_6\\_21-release](http://libexif.cvs.sourceforge.net/viewvc/libexif/libexif/NEWS?view=markup&pathrev=libexif-0_6_21-release)
- Référence CVE CVE-2012-2812 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2812>
- Référence CVE CVE-2012-2813 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2813>
- Référence CVE CVE-2012-2814 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2814>
- Référence CVE CVE-2012-2836 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2836>
- Référence CVE CVE-2012-2837 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2837>
- Référence CVE CVE-2012-2840 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2840>
- Référence CVE CVE-2012-2841 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2841>
- Référence CVE CVE-2012-2845 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2845>

### Gestion détaillée du document

17 juillet 2012 version initiale.