

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans FreeType

---

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-2010-AVI-359>

---

### Gestion du document

Référence	CERTA-2010-AVI-359-001
Titre	Multiples vulnérabilités dans FreeType
Date de la première version	09 août 2010
Date de la dernière version	19 août 2010
Source(s)	Liste des changements apportés à la version 2.4.2 de FreeType
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

- Dénis de service à distance ;
- exécution de code arbitraire à distance.

## 2 Systèmes affectés

FreeType versions 2.4.1 et antérieures.

## 3 Résumé

Plusieurs vulnérabilités présentes dans *FreeType* permettent à un utilisateur distant malintentionné de provoquer un déni de service ou d'exécuter du code arbitraire à distance.

## 4 Description

Plusieurs vulnérabilités sont présentes dans la bibliothèque de fonctions *FreeType* :

- la première (CVE-2010-1797) est relative au support des polices de caractères de type *Compact Font Format (CFF)* ;

- la seconde (CVE-2010-2805) concerne le traitement des polices de type *Adobe Type 1 Mac* (LWFN) ;
- la troisième (CVE-2010-2806) est due à une erreur dans le traitement des polices de type *T42* ;
- la quatrième (CVE-2010-2807) est relative à la mise en œuvre de la macro-commande *BOUNDS* incluse dans certaines polices ;
- la dernière (CVE-2010-2808) est liée à une erreur dans une fonction (*FT\_Stream\_EnterFrame()*) utilisée dans le traitement de certaines polices.

Toutes ces vulnérabilités permettent à un utilisateur distant malintentionné de provoquer un déni de service ou d'exécuter du code arbitraire.

## 5 Solution

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

## 6 Documentation

- Liste des changements apportés à la version 2.4.2 de FreeType :  
<http://freetype.sourceforge.net/index2.html#release-freetype-2.4.2>
- Bulletin de sécurité RedHat RHSA-2010:0607 du 05 août 2010 :  
<http://rhn.redhat.com/errata/RHSA-2010-0607.html>
- Bulletin de sécurité Ubuntu USN-972-1 du 17 août 2010 :  
<https://www.ubuntu.com/usn/usn-972-1>
- Référence CVE CVE-2010-1797 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1797>
- Référence CVE CVE-2010-2805 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2805>
- Référence CVE CVE-2010-2806 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2806>
- Référence CVE CVE-2010-2807 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2807>
- Référence CVE CVE-2010-2808 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2808>

## Gestion détaillée du document

**09 août 2010** version initiale.

**19 août 2010** ajout du bulletin Ubuntu.