



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité
des systèmes d'information
CERTA

Paris, le 16 juillet 2010
N° CERTA-2010-AVI-315

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : 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-315>

Gestion du document

Référence	CERTA-2010-AVI-315
Titre	Vulnérabilités dans FreeType
Date de la première version	16 juillet 2010
Date de la dernière version	–
Source(s)	Notes de la version 2.4.0 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

Exécution de code arbitraire à distance.

2 Systèmes affectés

FreeType versions 2.3.12 et antérieures.

3 Résumé

Plusieurs vulnérabilités dans *FreeType* permettent l'exécution de code arbitraire à distance.

4 Description

Plusieurs vulnérabilités dans la gestion des polices de *FreeType* ont été découvertes. Un attaquant peut, par le biais d'un fichier de police de caractères, provoquer l'exécution de code arbitraire à distance.

5 Solution

Mettre *FreeType* à jour en version 2.4.0.

6 Documentation

- Notes de la version 2.4.0 de FreeType :
<http://sourceforge.net/projects/freetype/files/freetype2/2.4.0/NEWS/view>
- Référence CVE CVE-2010-2497 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2497>
- Référence CVE CVE-2010-2498 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2498>
- Référence CVE CVE-2010-2499 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2499>
- Référence CVE CVE-2010-2500 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2500>
- Référence CVE CVE-2010-2519 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2519>
- Référence CVE CVE-2010-2520 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2520>

Gestion détaillée du document

16 juillet 2010 version initiale.