

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité 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-2007-AVI-226>

Gestion du document

Référence	CERTA-2007-AVI-226-002
Titre	Vulnérabilité dans FreeType
Date de la première version	24 mai 2007
Date de la dernière version	06 août 2007
Source(s)	Référence CVE CVE-2007-2754
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 2.3.4 et antérieures.

3 Résumé

Une vulnérabilité dans *FreeType* permet l'exécution de code arbitraire à distance.

4 Description

Une vulnérabilité a été découverte dans *FreeType* concernant le traitement des polices au format TTF. Un utilisateur mal intentionné peut, par le biais d'une police au format TTF spécifiquement constituée, exécuter du code arbitraire à distance.

5 Solution

Appliquer le correctif de FreeType (voir Documentation).

6 Documentation

- Correctif de *FreeType* :
<http://cvs.savannah.nongnu.org/viewvc/freetype2/src/truetype/ttgload.c?root=freetype&r1=1.177&r2=1.178>
- Bulletin sécurité Gentoo GLSA-200707-02 du 02 juillet 2007 :
<http://www.gentoo.org/security/en/glsa/glsa-200707-02.xml>
- Bulletin de sécurité Gentoo GLSA-200705-22 du 30 mai 2007 :
<http://www.gentoo.org/security/en/glsa/glsa-200705-22.xml>
- Bulletin sécurité Mandriva MDKSA-2007:121 du 13 juin 2007 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2007:121>
- Bulletin sécurité Red Hat RHSA-2007:0403 du 11 juin 2007 :
<http://www.redhat.com/errata/RHSA-2007-0403.html>
- Bulletin sécurité Debian DSA-1302 du 10 juin 2007 :
<http://www.debian.org/security/2007/dsa-1302>
- Bulletin sécurité Debian DSA-1454 du 7 janvier 2008 :
<http://www.debian.org/security/2007/dsa-1454>
- Bulletin sécurité SuSE SUSE-SA:2007:041 du 04 juillet 2007 :
<http://lists.opensuse.org/opensuse-security-announce/2007-07/msg00003.html>
- Bulletin de sécurité Ubuntu USN-466-1 du 30 mai 2007 :
<http://www.ubuntu.com/usn/usn-466-1>
- Bulletin sécurité Avaya ASA-2007-330 du 01 août 2007 :
<http://support.avaya.com/elmodocs2/security/ASA-2007-330.htm>
- Bulletin de sécurité Sun Solaris 103171 du 6 janvier 2008 :
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-103171-1>
- Référence CVE CVE-2007-2754 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2754>

Gestion détaillée du document

24 mai 2007 version initiale.

01 juin 2007 ajout des références aux bulletins de sécurité Gentoo, Ubuntu.

06 août 2007 ajout des références aux bulletins de sécurité des éditeurs.