



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 05 décembre 2007
N° CERTA-2007-AVI-517

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Cairo

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-517>

Gestion du document

Référence	CERTA-2007-AVI-517
Titre	Vulnérabilité de Cairo
Date de la première version	05 décembre 2007
Date de la dernière version	–
Source(s)	Rapport d'erreur RedHat #387431
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

Cairo versions 1.4.11 et antérieures.

3 Résumé

Une vulnérabilité dans Cairo permet à un utilisateur distant de provoquer un déni de service ou d'exécuter du code arbitraire à distance.

4 Description

Une vulnérabilité est présente dans la bibliothèque de fonctions d'affichage Cairo. Elle est relative à la mise en œuvre de l'affichage d'images au format PNG (Portable Network Graphics). Cette faille permet à un utilisateur distant de provoquer un déni de service de l'application utilisant Cairo ou l'exécution de code arbitraire. L'attaque peut être conduite à distance par le biais d'une image PNG construite de façon particulière.

5 Solution

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

6 Documentation

- Bulletin de sécurité Cairo du 27 novembre 2007 :
<http://cairographics.org/news/cairo-1.4.12>
- Rapport d'erreur RedHat #387431 :
https://bugzilla.redhat.org/show_bug.cgi?id=387431
- Bulletin de sécurité RedHat RHSA-2007:1078 du 29 novembre 2007 :
<http://rhn.redhat.com/errata/RHSA-2007-1078.html>
- Bulletin de sécurité Ubuntu USN-550-1 du 03 décembre 2007 :
<http://www.ubuntulinux.org/usn/usn-550-1>
- Référence CVE CVE-2007-5503 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5503>

Gestion détaillée du document

05 décembre 2007 version initiale.