Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 mars 2007
N° CERTA-2007-AVI-139

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de la bibliothèque ZZIPlib

Gestion du document

Référence	CERTA-2007-AVI-139
Titre	Vulnérabilité de la bibliothèque ZZIPlib
Date de la première version	27 mars 2007
Date de la dernière version	–
Source(s)	Notes de changement dans le projet du 17 mars 2007
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 ;
- contournement de la politique de sécurité.

2 Systèmes affectés

Les versions de la bibliothèque ZZIPlib antérieures à la 0.13.49.

3 Description

Une vulnérabilité a été identifiée dans la bilbiothèque ZZIPlib. Cette dernière fournit un accès en lecture pour les archives de type `ZIP`. Une erreur dans la fonction `zzip_open_shared_io` qui est mise en œuvre dans le fichier `zzip/file.c` permettrait à une personne malveillante de perturber le système vulnérable, voire exécuter des commandes arbitraires. De manière plus précise, un appel à la fonction `strcpy` ne serait pas correctement contrôlé, et la manipulation d'un nom de fichier trop long pourrait ainsi provoquer un débordement de tampon.

4 Solution

Se référer au bulletin de mise à jour du projet pour l'obtention des correctifs (cf. section Documentation).

5 Documentation

- Page du projet ZZIPlib :
  http://sourceforge.net/projects/zziplib/
- Notes de modifications pour la version 0.13.49 du 17 mars 2007 :
  http://sourceforge.net/project/shownotes.php?group_id=6389&release_id=494587
- Référence CVE CVE-2007-1614 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1614

Gestion détaillée du document

27 mars 2007 version initiale.