Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 novembre 2006
N° CERTA-2006-AVI-504

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de WinZip

Gestion du document

Référence	CERTA-2006-AVI-504
Titre	Vulnérabilité de WinZip
Date de la première version	17 novembre 2006
Date de la dernière version	–
Source(s)	Avis de mise à jour WinZip du 14 novembre 2006
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 WinZip antérieures à WinZip 10.0 Build 7245 (y compris la Pre Build 7245).

3 Résumé

Une vulnérabilité a été identifiée dans WinZip. Elle pourrait être exploitée localement ou à distance pour permettre l'exécution de code arbitraire sur la machine ayant une version vulnérable.

4 Description

Une vulnérabilité a été identifiée dans WinZip. Ce dernier, au cours de son installation, créée un contrôle ActiveX sur le système : `WZFILEVIEW.FileViewCtrl.61` (CLSID : A09AE68F-B14D-43ED-B713-BA413F034904).

Celui-ci contiendrait plusieurs fonctions qui ne seraient pas correctement sécurisées. Cependant, ce contrôle ActiveX est marqué "sain pour l'exécution" (*Safe for scripting*), ce qui indique à Internet Explorer par exemple que cet ActiveX peut être utilisé si une page Web visitée le demande. Nous rappelons à cet égard qu'il est fortement recommandé de désactiver les ActiveX au niveau du navigateur Internet Explorer. Cette vulnérabilité peut aussi être exploitée localement afin d'élever ses privilèges à ceux de l'administrateur.

5 Solution

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

6 Documentation

- Référence CVE CVE-2006-5198 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5198
- Avis de mise à jour WinZip du 14 novembre 2006 :
  http://www.winzip.com/wz7245.htm
- Avis de sécurité ZDI-06-040 de TippingPoint ZeroDayInitiative du14 novembre 2006 :
  http://www.zerodayinitiative.com/advisories/ZDI-06-040.html

Gestion détaillée du document

17 novembre 2006 version initiale.