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 mars 2004
N° CERTA-2004-AVI-056-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de WinZip

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-2004-AVI-056`

Gestion du document

Référence	CERTA-2004-AVI-056-002
Titre	Vulnérabilité de WinZip
Date de la première version	01 mars 2004
Date de la dernière version	16 mars 2004
Source(s)	Avis de sécurité iDEFENSE 02.27.04a
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

- Déni de service ;
- exécution de code arbitraire à distance.

2 Systèmes affectés

- WinZip FR version 8.1 SR-1 et versions antérieures ;
- WinZip US version 8.1 SR-1 et versions antérieures.

3 Résumé

Une vulnérabilité de WinZip dans la gestion des archives de type MIME permet à un utilisateur mal intentionné de réaliser un débordement de mémoire et ainsi d'exécuter du code arbitraire à distance.

4 Description

WinZip est un programme pour Microsoft Windows de gestion des archives aux formats tels que `CAB, TAR, gzip, UUencode, BinHex, et MIME`. Un débordement de mémoire dans la gestion des archives de type

MIME (fichiers d'extensions `.b64, .bhx, .hqx, .mim, .uu, .uue et .xxe`) permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance par l'intermédiaire d'une archive habilement constituée.

5 Contournement provisoire

Désactiver l'association entre WinZip et les fichiers d'extensions `.b64, .bhx, .hqx, .mim, .uu, .uue et .xxe`. Pour cela, dans le menu `Options` choisir `Configuration...`, dans l'onglet `Système` cliquer sur le bouton `Associations` et décocher les extensions `.B64, .BHX, .HQX, .MIM, .UU, .UUE et .XXE`.

6 Solution

Mettre à jour WinZip en version 8.1 SR-2.

- La page de téléchargement de la mise à jour pour la version FR se situe à l'adresse suivante :
  http://www.absoft.fr/FR/produits/Winzip/service_maj.asp
- La page de téléchargement de la mise à jour pour la version US se situe à l'adresse suivante :
  http://www.winzip.com/wz81sr2.htm

7 Documentation

- Site internet de WinZip :
  http://www.winzip.com
- Site internet de WinZip français :
  http://www.winzip.com/french.htm
  http://www.absoft.fr/FR/produits/Winzip/
- Avis de sécurité de WinZip Computing :
  http://www.winzip.com/fmwz90.htm
- Avis de sécurité iDEFENSE 02.27.04a :
  http://www.idefense.com/application/poi/display?id=76&type=vulnerabilites

Gestion détaillée du document

01 mars 2004 version initiale.

04 mars 2004 correction de l'avis pour prendre en compte la spécificité des versions localisées.

16 mars 2004 prise en compte du correctif WinZip 8.1 SR-2 (y compris WinZip FR).