

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de la commande UnZip

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-2003-AVI-138>

Gestion du document

Référence	CERTA-2003-AVI-138
Titre	Vulnérabilité de la commande UnZip
Date de la première version	20 août 2003
Date de la dernière version	–
Source(s)	Bulletin de sécurité DSA-344 de Debian Bulletin de sécurité RHSA-2003:199 de RedHat Bulletin de sécurité MDKSA-2003:071 de Mandrake
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

Atteinte à l'intégrité du système.

2 Systèmes affectés

Tous les systèmes possédant la version 5.50 (ou antérieure) de UnZip.

3 Description

Lors de l'extraction des fichiers contenus dans une archive au format `.zip`, le chemin des fichiers n'est pas correctement validé.

Il est alors possible, pour un utilisateur mal intentionné, de constituer une archive contenant des fichiers qui seront extraits dans un répertoire parent du répertoire d'extraction initial (présence de la séquence `./` dans le chemin d'accès).

4 Solution

Appliquer le correctif de l'éditeur :

- Bulletin de sécurité DSA-344 de Debian :
<http://www.debian.org/security/2003/dsa-344>
- Bulletin de sécurité MDKSA-2003:073 de Mandrake :
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:073>
- Bulletin de sécurité RHSA-2003:199 de Red Hat :
<http://rhn.redhat.com/errata/RHSA-2003-199.html>

5 Documentation

- Site Info-Zip :
<http://www.info-zip.org/pub/infozip/UnZip.html>
- Référence CVE CAN-2003-0282
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0282>

Gestion détaillée du document

20 août 2003 version initiale.