

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans l'utilitaire 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-2005-AVI-434>

Gestion du document

Référence	CERTA-2005-AVI-434-001
Titre	Vulnérabilité dans l'utilitaire unzip
Date de la première version	03 novembre 2005
Date de la dernière version	21 novembre 2005
Source(s)	Bulletin de sécurité Mandriva MDKSA-2005:197 du 26 octobre 2005
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

Elevation de privilèges.

2 Systèmes affectés

Unzip 5.52 et versions antérieures.

3 Résumé

Deux vulnérabilités dans l'utilitaire unzip permet à un utilisateur local mal intentionné d'élever ses privilèges.

4 Description

Unzip est un utilitaire de décompression d'archive.

- Une vulnérabilité affectant la version 5.51 et versions antérieures d'unzip permet à un utilisateur local mal intentionné d'élever ses privilèges (CAN-2005-0602);
- une seconde vulnérabilité affectant cette fois la version 5.52 d'unzip ainsi que les versions antérieures permet à un individu malveillant d'élever ses privilèges (CAN-2005-2475).

5 Solution

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

6 Documentation

- Bulletin de sécurité Mandriva MDKSA-2005:197 du 26 octobre 2005 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2005:197>
- Bulletin de sécurité Ubuntu USN-191-1 du 29 septembre 2005 :
<http://www.ubuntu.com/usn/usn-191-1/>
- Bulletin de sécurité Debian DSA-903 du 21 novembre 2005 :
<http://www.debian.org/security/2005/dsa-903>
- Référence CVE CAN-2005-0602 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0602>
- Référence CVE CAN-2005-2475 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2475>

Gestion détaillée du document

03 novembre 2005 version initiale.

21 novembre 2005 ajout des références aux bulletins de sécurité Debian et Ubuntu.