

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de GNU Midnight Commander

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-146>

Gestion du document

Référence	CERTA-2004-AVI-146-005
Titre	Vulnérabilité de GNU Midnight Commander
Date de la première version	30 avril 2004
Date de la dernière version	01 juin 2004
Source(s)	Avis de sécurité Debian DSA-497
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

Toutes les versions de GNU Midnight Commander (mc).

3 Résumé

Plusieurs vulnérabilités dans GNU Midnight Commander (mc) permettent à un utilisateur mal intentionné de réaliser un déni de service ou d'exécuter du code arbitraire à distance.

4 Description

GNU Midnight Commander (mc) est un gestionnaire de fichiers destiné aux systèmes d'exploitation libres. Plusieurs vulnérabilités ont été découvertes :

- Multiples vulnérabilités de type débordement de mémoire (CAN-2004-0226) ;

- une vulnérabilité de type chaîne de format (CAN-2004-0232) ;
- une vulnérabilité dans la création des fichiers et répertoires temporaires (CAN-2004-0231).

Ces vulnérabilités permettent à un utilisateur mal intentionné de réaliser un déni de service ou d'exécuter du code arbitraire à distance sur la machine victime.

5 Solution

Appliquer le correctif fourni par votre éditeur (cf. section Documentation).

6 Documentation

- Site Internet de GNU Midnight Commander :
<http://www.ibiblio.org/mc/>
- Avis de sécurité Debian DSA-497 :
<http://www.debian.org/security/2004/dsa-497>
- Avis de sécurité Mandrake MDKSA-2004:039 :
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:039>
- Avis de sécurité RedHat
 - Red Hat Enterprise et Advanced Workstation RHSA-2004:172 :
<http://rhn.redhat.com/errata/RHSA-2004-172.html>
 - Red Hat 9 RHSA-2004:173 :
<http://rhn.redhat.com/errata/RHSA-2004-173.html>
- Avis de sécurité SUSE SuSE-SA:2004:012 du 14 mai 2004 :
http://www.suse.com/de/security/2004_12_mc.html
- Avis de sécurité Gentoo GLSA 200405-21 du 26 mai 2004 :
<http://www.gentoo.org/security/en/glsa/glsa-200405-21.xml>
- Avis de sécurité FreeBSD du 02 mai 2004 :
<http://www.vuxml.org/freebsd/>
- Référence CVE CAN-2004-0226 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0226>
- Référence CVE CAN-2004-0231 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0231>
- Référence CVE CAN-2004-0232 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0232>

Gestion détaillée du document

30 avril 2004 version initiale.

03 mai 2004 ajout de l'avis de sécurité RedHat.

12 mai 2004 ajout de la référence au bulletin de sécurité FreeBSD.

17 mai 2004 ajout de la référence au bulletin de sécurité SUSE.

26 mai 2004 ajout référence au bulletin de sécurité Red Hat Enterprise.

01 juin 2004 ajout référence au bulletin de sécurité Gentoo.