

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de 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-2005-AVI-081>

Gestion du document

Référence	CERTA-2005-AVI-081-002
Titre	Vulnérabilité de Midnight Commander
Date de la première version	18 février 2005
Date de la dernière version	17 juin 2005
Source(s)	Bulletin de sécurité Gentoo GLSA 200502-24
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 de type débordement de mémoire ont été découvertes dans GNU Midnight Commander (mc).

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

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

6 Documentation

- Site Internet de GNU Midnight Commander :
<http://www.ibiblio.org/mc/>
- Bulletin de sécurité Gentoo GLSA 200502-24 du 17 février 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200502-24.xml>
- Bulletin de sécurité RedHat RHSA-2005:217 du 04 mars 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-217.html>
- Bulletin de sécurité RedHat RHSA-2005:512 du 16 juin 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-512.html>
- Bulletin de sécurité OpenBSD pour mc du 17 février 2005 :
<http://www.vuxml.org/openbsd/>
- Bulletin de sécurité Debian DSA-639 du 14 janvier 2005 :
<http://www.debian.org/security/2005/dsa-639>
- Bulletin de sécurité Debian DSA-698 du 29 mars 2005 :
<http://www.debian.org/security/2005/dsa-698>
- Référence CVE CAN-2004-1004 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1004>
- Référence CVE CAN-2004-1005 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1005>
- Référence CVE CAN-2004-1009 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1009>
- Référence CVE CAN-2004-1090 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1090>
- Référence CVE CAN-2004-1091 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1091>
- Référence CVE CAN-2004-1092 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1092>
- Référence CVE CAN-2004-1093 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1093>
- Référence CVE CAN-2004-1174 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1174>
- Référence CVE CAN-2004-1175 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1175>
- Référence CVE CAN-2004-1176 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1176>
- Référence CVE CAN-2005-0763 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0763>

Gestion détaillée du document

18 février 2005 version initiale.

07 mars 2005 ajout de la référence au bulletin de sécurité RedHat RHSA-2005:217.

17 juin 2005 ajout des références aux bulletins de sécurité Debian DSA-639, Debian DSA-698 et RedHat RHSA-2005:512. Ajout des références CVE CAN-2004-1009, CAN-2004-1090, CAN-2004-1091, CAN-2004-1093, CAN-2004-1174, CAN-2004-1175 et CVE CAN-2005-0763.