

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de mpg123

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-304>

Gestion du document

Référence	CERTA-2004-AVI-304-004
Titre	Vulnérabilité de mpg123
Date de la première version	08 septembre 2004
Date de la dernière version	15 octobre 2004
Source(s)	Bulletin de sécurité de Davide Del Vecchio Adv#10
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

Exécution de code arbitraire.

2 Systèmes affectés

mpg123 version 0.59r et versions antérieures.

3 Résumé

Une vulnérabilité dans mpg123 permet à un utilisateur mal intentionné d'exécuter du code arbitraire sur la plate-forme vulnérable.

4 Description

mpg123 est un lecteur de fichiers MPEG Layer 1, 2 et 3 pour les systèmes UNIX.
Une vulnérabilité dans mpg123 permet à un utilisateur mal intentionné, via un fichier habilement constitué, d'exécuter du code arbitraire avec les privilèges de l'utilisateur lisant le fichier.

5 Solution

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

6 Documentation

- Site Internet du lecteur mpg123 :
<http://www.mpg123.de>
- Bulletin de sécurité de Davide Del Vecchio Adv#10 :
<http://www.alighieri.org/advisories/advisory-mpg123.txt>
- Bulletin de sécurité FreeBSD pour mpg123 du 14 septembre 2004 :
<http://www.vuxml.org/freebsd/>
- Mise à jour de sécurité des paquetages NetBSD mpg123, mpg123-esound et mpg123-nas :
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/audio/mpg123/README.html>
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/audio/mpg123-esound/README.html>
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/audio/mpg123-nas/README.html>
- Bulletin de sécurité Gentoo GLSA-200409-20.xml du 16 septembre 2004 :
<http://www.gentoo.org/security/en/glsa/glsa-200409-20.xml>
- Bulletin de sécurité Mandrake MDKSA-2004:100 du 22 septembre 2004 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:100>
- Bulletin de sécurité debian DSA-564 du 13 octobre 2004 :
<http://www.debian.org/security/2004/dsa-564>
- Référence CVE CAN-2004-0805 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0805>

Gestion détaillée du document

08 septembre 2004 version initiale.

14 septembre 2004 ajout de la référence au bulletin de sécurité FreeBSD.

17 septembre 2004 ajout de la référence au bulletin de sécurité Gentoo.

23 septembre 2004 ajout de la référence au bulletin de sécurité Mandrake.

15 octobre 2004 ajout de la référence au bulletin de sécurité Debian.