Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 03 janvier 2005
N° CERTA-2004-AVI-414-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans MPlayer

Gestion du document

Référence	CERTA-2004-AVI-414-002
Titre	Vulnérabilités dans MPlayer
Date de la première version	22 décembre 2004
Date de la dernière version	03 janvier 2005
Source(s)	Avis de sécurité sur le site de MPlayer
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 à distance.

2 Systèmes affectés

MPlayer version 1.0pre5.

3 Description

Trois vulnérabilités ont été découvertes dans le lecteur vidéo MPlayer.

La première vulnérabilité nécessite la connexion à un serveur malicieux. En incitant un utilisateur à se connecter à un tel serveur, il est possible d'exécuter du code arbitraire à distance.

Les deux autres vulnérabilités permettent, par le biais d'un fichier habilement constitué, l'exécution de code arbitraire à distance avec les droits de l'utilisateur qui visualise le fichier.

4 Solution

Se référer au site de MPlayer pour l'obtention des correctifs (cf. section Documentation)

5 Documentation

- Site Internet de MPlayer :
  http://www.mplayerhq.hu
- Bulletin de sécurité 166 d'iDefense du 16 décembre 2004 :
  http://www.idefense.com/application/poi/display?id=166&type=vulnerabilities
- Bulletin de sécurité 167 d'iDefense du 16 décembre 2004 :
  http://www.idefense.com/application/poi/display?id=167&type=vulnerabilities
- Bulletin de sécurité 168 d'iDefense du 16 décembre 2004 :
  http://www.idefense.com/application/poi/display?id=168&type=vulnerabilities
- Bulletin de sécurité Mandrake MDKSA-2004:157 du 22 décembre 2004 :
  http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:157
- Bulletin de sécurité Gentoo GLSA-200412-21 du 20 décembre 2004 :
  http://www.gentoo.org/security/en/glsa/glsa-200412-21.xml
- Bulletin de sécurité FreeBSD "mplayer – multiple vulnerabilities" du 21 décembre 2004 :
  http://www.vuxml.org/freebsd/
- Bulletin de sécurité OpenBSD "mplayer – multiple overflow vulnerabilites" du 22 décembre 2004 :
  http://www.vuxml.org/openbsd/
- Référence CVE CAN-2004-1309 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1309
- Référence CVE CAN-2004-1310 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1310
- Référence CVE CAN-2004-1311 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1311

Gestion détaillée du document

22 décembre 2004 version initiale.

23 décembre 2004 ajout références aux bulletins de sécurité Mandrake, FreeBSD et OpenBSD. Ajout références CVE.

03 janvier 2005 ajout référence au bulletin de sécurité Gentoo.