



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 juillet 2005
N° CERTA-2005-AVI-153-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de MPlayer

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-153>

Gestion du document

Référence	CERTA-2005-AVI-153-001
Titre	Multiples vulnérabilités de MPlayer
Date de la première version	21 avril 2005
Date de la dernière version	12 juillet 2005
Source(s)	Bulletin de sécurité Gentoo
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

MPlayer versions 1.0pre6 et antérieures.

3 Description

Deux vulnérabilités de type débordement de mémoire sont présentes dans la lecture des flux MMST et RTSP. En incitant un utilisateur à se connecter à un serveur malicieusement construit, il est possible de réaliser l'exécution de code arbitraire à distance sur un système utilisant un lecteur MPlayer vulnérable.

4 Solution

La version 1.0pre7 de MPlayer corrige ces vulnérabilités.

5 Documentation

- Site Internet de MPlayer :
<http://www.mplayerhq.hu>
- Bulletin de sécurité MPlayer du 16 avril 2005 (#vuln 10) :
<http://www.mplayerhq.hu/homepage/design7/news.html#vuln10>
- Bulletin de sécurité MPlayer du 16 avril 2005 (#vuln 11) :
<http://www.mplayerhq.hu/homepage/design7/news.html#vuln11>
- Bulletin de sécurité Gentoo GLSA-200504-19 du 20 avril 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200504-19.xml>
- Bulletin de sécurité Mandriva MDKSA-2005:115 du 11 juillet 2005 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2005:115>

Gestion détaillée du document

21 avril 2005 version initiale.

12 juillet 2005 ajout des bulletins de sécurité MPlayer (#vuln 10 et #vuln 11) et du bulletin de sécurité Mandriva MDKSA-2005:115.