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 mai 2004
N° CERTA-2004-AVI-107-003

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans MPlayer

Gestion du document

Référence	CERTA-2004-AVI-107-003
Titre	Vulnérabilité dans MPlayer
Date de la première version	02 avril 2004
Date de la dernière version	12 mai 2004
Source(s)	Avis de sécurité MPLAYERHQ.HU
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 0.90pre series ;
- MPlayer 0.90rc series ;
- MPlayer 0.90 ;
- MPlayer 0.91 ;
- MPlayer 1.0pre1 ;
- MPlayer 1.0pre2 ;
- MPlayer 1.0pre3.

3 Résumé

Une vulnérabilité a été découverte dans certaines versions de MPlayer.

4 Description

MPlayer est un lecteur multimédia fonctionnant sous Linux. Une vulnérabilité a été découverte dans la mise en œuvre de la fonction de traitement des entêtes HTTP :
`http_build_request()`. Cette vulnérabilité peut être exploitée par un utilisateur mal intentionné, via une page d'un site malicieux, afin d'exécuter du code arbitraire sur la machine.

5 Solution

Appliquer le correctif fourni par l'éditeur (cf. Documentation).

6 Documentation

- Avis de sécurité MPLAYERHQ.HU :
  http://mp.dev.hu/homepage/design6/news.html
- Avis de sécurité Gentoo GLSA 200403-13 :
  http://www.gentoo.org/security/en/glsa/glsa-200403-13.xml
- Bulletin de sécurité Mandrake MDKSA-2004:026 :
  http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:026
- Correctif de la vulnérabilité :
  http://mp.dev.hu/MPlayer/patches/vuln02-fix.diff
- Avis de sécurité FreeBSD du 31 mars 2004 :
  http://www.vuxml.org/freebsd/
- Avis de sécurité pour le paquetage OpenBSD mplayer du 30 mars 2004 :
  http://www.vuxml.org/openbsd/
- Mise à jour de sécurité du paquetage NetBSD mplayer :
  ftp://ftp.netbsd.org/pub/NetBSD/packages/distfiles/vulnerabilities
- Référence CVE CAN-2004-0386 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0386

Gestion détaillée du document

02 avril 2004 version initiale.
06 avril 2004 ajout référence au bulletin de sécurité de Mandrake.
10 mai 2004 ajout de la référence CVE.
12 mai 2004 ajout des références aux bulletins de sécurité FreeBSD, OpenBSD et NetBSD.