Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 février 2008
N° CERTA-2008-AVI-045-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans MPlayer et xine-lib

Gestion du document

Référence	CERTA-2008-AVI-045-001
Titre	Vulnérabilités dans MPlayer et xine-lib
Date de la première version	05 février 2008
Date de la dernière version	13 février 2008
Source(s)	Avis de sécurité pour MPlayer du 29 et 30 janvier 2008
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 versions 1.0rc2 et antérieures ;
- Xine-lib versions 1.1.10 et antérieures.

3 Résumé

De multiples vulnérabilités affectant MPlayer permettent à une personne malintentionnée d'exécuter du code arbitraire à distance.

4 Description

De multiples vulnérabilités de type débordement de mémoire ont été identifiées dans `MPlayer`, dans les fichiers *demux_audio.c*, *demux_mov.c*, *url.c*, et *stream_cddb.c*. Une personne malintentionnée peut ainsi exécuter du code arbitraire à distance, en incitant par exemple un utilisateur à ouvrir un fichier spécifiquement construit.

La première vulnérabilité se situe en fait dans la bibliothèque `xine-lib`, et sa fonction *open_flac_file()* utilisée pour traiter des fichiers de type `FLAC`. D'autres produits utilisant cette bibliothèque peuvent être affectés.

5 Solution

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

6 Documentation

- Site de l'éditeur :
  http://www.mplayerhq.hu/design7/news.html
- Bulletin de sécurité Debian DSA-1496 du 12 février 2008 :
  http://lists.debian.org/debian-security-announce/debian-security-announce-2008/msg00058.html
- Référence CVE CVE-2008-0485 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0485
- Référence CVE CVE-2008-0486 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0486
- Référence CVE CVE-2008-0629 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0629
- Référence CVE CVE-2008-0630 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0630

Gestion détaillée du document

05 février 2008 version initiale ;
13 février 2008 ajout de références CVE et du bulletin de sécurité Debian.