

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans 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-2008-AVI-221>

Gestion du document

Référence	CERTA-2008-AVI-221-001
Titre	Vulnérabilité dans mplayer
Date de la première version	21 avril 2008
Date de la dernière version	18 septembre 2008
Source(s)	Bulletin de sécurité Debian DSA-1552 du 19 avril 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 1.x.

3 Résumé

Une vulnérabilité découverte dans le lecteur multimédia MPlayer permet à un utilisateur malintentionné d'exécuter du code arbitraire à distance.

4 Description

Une vulnérabilité présente dans la fonction `sdpplin_parse()` du fichier `sdpplin.c` peut être exploitée, au moyen du paramètre `StreamCount` du protocole SDP (Session Description Protocol), lorsqu'il est renseigné de façon particulière ; de cette façon, une personne malveillante peut exécuter du code arbitraire à distance.

5 Solution

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

6 Documentation

- Bulletin de sécurité Debian DSA 1552 du 19 avril 2008 :
<http://www.debian.org/security/2008/dsa-1552>
- Bulletin de sécurité Gentoo GLSA-200805-22 du 29 mai 2008 :
<http://www.gentoo.org/security/en/glsa/glsa-200805-22.xml>
- Bulletin de sécurité Mandriva MDVSA-2008:196 du 15 septembre 2008 :
<http://www.mandriva.com/en/security/advisories?name=MDVSA-2008:196>
- Référence CVE CVE-2008-1558 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1558>

Gestion détaillée du document

21 avril 2008 version initiale.

18 septembre 2008 ajout des références aux bulletins de sécurité Gentoo et Mandriva.