



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 01 juin 2004
N° CERTA-2004-AVI-152-003

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de MPlayer et Xine

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-2004-AVI-152>

Gestion du document

Référence	CERTA-2004-AVI-152-003
Titre	Vulnérabilité de MPlayer et Xine
Date de la première version	03 mai 2004
Date de la dernière version	01 juin 2004
Source(s)	Avis de sécurité Xine XSA-2004-3
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 1.0pre1-pre3try2 ;
- xine-lib versions 1-beta1 à 1-rc3c.

3 Résumé

Plusieurs vulnérabilités ont été découvertes dans MPlayer et Xine permettant à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

4 Description

MPlayer et Xine sont des lecteurs multimedia open-source. RTSP (Real-Time Streaming Protocol) est un protocole de gestion de flux multimedia utilisé notamment pour communiquer avec les serveurs RealNetworks. MPlayer et Xine partagent le même code source quant à la gestion du protocole RTSP.

Plusieurs vulnérabilités ont été découvertes dans le code gérant le protocole RTSP permettant à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

5 Solution

- Mettre à jour MPlayer en version 1.0pre4. Site Internet de téléchargement de MPlayer :
<http://www.mplayerhq.hu/homepage/dload.html>
- Mettre à jour xine-lib en version 1-rc4. Site Internet de téléchargement de xine-lib :
<http://xinehq.de/index.php/releases>

6 Documentation

- Avis de sécurité MPlayer du 28 avril 2004 :
<http://www.mplayerhq.hu/homepage/design7/news.html>
- Avis de sécurité Xine XSA-2004-3 du 25 avril 2004 :
<http://xinehq.de/index.php/security/XSA-2004-3>
- Avis de sécurité SUSE SuSE-SA:2004:012 du 14 mai 2004 :
http://www.suse.com/de/security/2004_12_mc.html
- Avis de sécurité Gentoo GLSA 200405-24 du 01 juin 2004 :
<http://www.gentoo.org/security/en/glsa/glsa-200405-24.xml>
- Avis de sécurité pour le paquetage OpenBSD mplayer du 06 mai 2004 :
<http://www.vuxml.org/openbsd/>
- Mise à jour de sécurité des paquetages NetBSD mplayer et xine-lib :
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/multimedia/mplayer/README.html>
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/multimedia/xine-lib/README.html>
- Référence CVE CAN-2004-0433 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0433>

Gestion détaillée du document

03 mai 2004 version initiale.

12 mai 2004 ajout des références aux bulletins de sécurité OpenBSD et NetBSD.

17 mai 2004 correction des références aux bulletins de sécurité NetBSD, ajout du bulletin de sécurité de SUSE.

01 juin 2004 ajout de la référence au bulletin de sécurité Gentoo et de la référence CVE.