

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans VLC

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-2009-AVI-296>

Gestion du document

Référence	CERTA-2009-AVI-296-001
Titre	Vulnérabilité dans VLC
Date de la première version	28 juillet 2009
Date de la dernière version	30 juillet 2009
Source(s)	Correctif apporté dans la dernière version de VLC
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

VLC versions 1.0.0 et antérieures.

3 Résumé

Une vulnérabilité dans VLC permet à un utilisateur distant d'exécuter du code arbitraire.

4 Description

Une vulnérabilité de type débordement d'entier est présente dans le lecteur multimedia VLC. Elle est relative à la mise en œuvre du support des flux au format RTSP (Real Time Streaming Protocol) et permet à un utilisateur distant malintentionné d'exécuter du code arbitraire via un flux RTSP particulier.

5 Solution

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

La version 1.0.1 corrige le problème :

<http://download.videolan.org/pub/videolan/vlc/1.0.1/>

6 Documentation

- Site de VLC :
<http://videolan.org>
- Liste des changements apportés à la version 1.0.1 de VLC :
<http://wiki.videolan.org/Changelog/1.0.1/>
- Correctif apporté à la dernière version de VLC :
<http://git.videolan.org/?p=vlc.git;a=commitdiff;h=dc74600c97eb834c08674676e209afa842053aca>

Gestion détaillée du document

28 juillet 2009 version initiale.

30 juillet 2009 ajout du lien vers la liste des changements apportés à la version 1.0.1.