Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 décembre 2007
N° CERTA-2007-AVI-568

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans VLC Media Player

Gestion du document

Référence	CERTA-2007-AVI-568
Titre	Multiples vulnérabilités dans VLC Media Player
Date de la première version	27 décembre 2007
Date de la dernière version	–
Source(s)	–
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 Media Player version 0.8.6d et les versions antérieures.

3 Résumé

Des vulnérabilités affectant VLC Media Player ont été découvertes et permettent d'exécuter du code arbitraire à distance.

4 Description

De multiples vulnérabilités dans VLC Media Player permettent d'exécuter du code arbitraire à distance :

– des erreurs dans certaines fonctions entrant dans la gestion des sous-titres peuvent provoquer un dépassement de la mémoire tampon ;

– une erreur dans l'interface web en écoute sur le port 8080 (désactivée par défaut) peut être exploitée via une requête HTTP spécialement conçue.

5 Solution

Se référer au site de VLC pour l'obtention des correctifs (cf. section Documentation).

Ce dernier est, à la date de rédaction de cet avis, uniquement disponible dans la branche de développement de VLC.

Le CERTA tient à rappeler que les versions en cours de développement peuvent comporter d'autres vulnérabilités et conseille l'utilisation d'un lecteur alternatif en attendant que le correctif soit intégré dans la version stable du logiciel.

6 Documentation

– Le site de la branche développement de VLC :
http://nightlies.videolan.org
– L'actualité du projet VLC :
http://www.videolan.org/news.html#news-1

Gestion détaillée du document

27 décembre 2007 version initiale.