

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités 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-2008-AVI-295>

Gestion du document

Référence	CERTA-2008-AVI-295
Titre	Multiples vulnérabilités dans VLC
Date de la première version	09 juin 2008
Date de la dernière version	–
Source(s)	Notes de version VLC 0.8.6h
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 ;
- déni de service à distance.

2 Systèmes affectés

VLC versions 0.8.6g et antérieures.

3 Résumé

De multiples vulnérabilités dans VLC permettent de réaliser un déni de service ou d'exécuter du code arbitraire à distance.

4 Description

VLC intègre des versions vulnérables de *GnuTLS*, de *libcrypt* (CVE-2008-1948, CVE-2008-1949 et CVE-2008-1950) et de *libxml2* (CVE-2007-6284) pour *Windows* et *Mac OS X*.

L'exploitation de ces vulnérabilités (traitées par les avis CERTA-2008-AVI-022 et CERTA-2008-AVI-262) permet de réaliser un déni de service ou d'exécuter du code arbitraire à distance.

5 Solution

Mettre à jour VLC en version 0.8.6h.

6 Documentation

- Notes de changement de version VLC 0.8.6h :
<http://wiki.videolan.org/Changelog/0.8.6h>
- Téléchargement de VLC :
<http://www.videolan.org/vlc/>
- Avis CERTA-2008-AVI-022 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-022/>
- Avis CERTA-2008-AVI-262 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-262/>
- Référence CVE CVE-2007-6284 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6284>
- Référence CVE CVE-2008-1948 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1948>
- Référence CVE CVE-2008-1949 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1949>
- Référence CVE CVE-2008-1950 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1950>

Gestion détaillée du document

09 juin 2008 version initiale.