Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 mars 2006
N° CERTA-2005-AVI-499-004

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans la bibliothèque libavcodec de FFmpeg

Gestion du document

Référence	CERTA-2005-AVI-499-004
Titre	Vulnérabilité dans la bibliothèque libavcodec
Date de la première version	22 décembre 2005
Date de la dernière version	17 mars 2006
Source(s)	Liste de diffusion BugTraq
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

- Déni de service ;
- exécution de code arbitraire à distance.

2 Systèmes affectés

- FFmpeg versions 0.x ;
- Xline-lib 1.x.

3 Résumé

Une vulnérabilité présente dans la bibliothèque `libavcodec` de `FFmpeg` peut être exploitée par un utilisateur mal intentionné pour réaliser un déni de service ou exécuter du code arbitraire à distance.

4 Description

La bibliothèque `libavcodec` est le composant chargé de la compression et de la décompression dans divers formats (mpeg, png...).

Une vulnérabilité présente dans la fonction `avcodec_default_get_buffer` du programme `utils.c` de cette bibliothèque peut être exploitée par un utilisateur mal intentionné pour réaliser un deni de service ou pour exécuter du code arbitraire à distance à partir d'un fichier au format `png` malicieusement construit.

5 Solution

Appliquer les correctifs disponibles sur le site de votre éditeur.

6 Documentation

- Bulletin de sécurité Ubuntu USN-230-2 :
  http://www.ubuntulinux.org/usn/usn-230-2/
- Bulletin de sécurité Mandriva MDKSA-2005:228 pour xine-lib du 14 décembre 2005 :
  http://frontal2.mandriva.com/security/advisories?name=MDKSA-2005:228
- Bulletin de sécurité Mandriva MDKSA-2005:229 pour xmovie du 14 décembre 2005 :
  http://frontal2.mandriva.com/security/advisories?name=MDKSA-2005:229
- Bulletin de sécurité Mandriva MDKSA-2005:230 pour mplayer du 14 décembre 2005 :
  http://frontal2.mandriva.com/security/advisories?name=MDKSA-2005:230
- Bulletin de sécurité Mandriva MDKSA-2005:231 pour ffmpeg du 14 décembre 2005:
  http://frontal2.mandriva.com/security/advisories?name=MDKSA-2005:231
- Bulletin de sécurité Mandriva MDKSA-2005:232 pour gestreamer-ffmpeg du 14 décembre 2005 :
  http://frontal2.mandriva.com/security/advisories?name=MDKSA-2005:232
- Bulletin de sécurité Gentoo GLSA 200601-06 du 10 janvier 2006 :
  http://www.gentoo.org/security/en/glsa/glsa-200601-06.xml
- Bulletin de sécurité Gentoo GLSA 200602-01 du 05 février 2006 :
  http://www.gentoo.org/security/en/glsa/glsa-200602-01.xml
- Bulletin de sécurité Gentoo GLSA 200603-03 du 04 mars 2006 :
  http://www.gentoo.org/security/en/glsa/glsa-200603-03.xml
- Bulletin de sécurité Debian DSA-992 du 10 mars 2006 :
  http://www.debian.org/security/2006/dsa-992
- Bulletin de sécurité Debian DSA-1004 du 16 mars 2006 :
  http://www.debian.org/security/2006/dsa-1004
- Bulletin de sécurité Debian DSA-1005 du 16 mars 2006 :
  http://www.debian.org/security/2006/dsa-1005
- Référence CVE CAN-2005-4048 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-4048

7 Documentation

Gestion détaillée du document

22 décembre 2005 version initiale.
16 janvier 2006 ajout des références aux bulletins de sécurité Mandriva et Gentoo 200601-06.
08 mars 2006 ajout de la référence aux bulletin de sécurité Gentoo 200603-03.
10 mars 2006 ajout de la référence au bulletin de sécurité Debian DSA-992.
17 mars 2006 ajout des références aux bulletins de sécurité Gentoo 200602-01, Debian DSA-1004 et DSA-1005.