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 juin 2006
N° CERTA-2006-AVI-255

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Real Helix RTSP

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-2006-AVI-255

Gestion du document

Référence	CERTA-2006-AVI-255
Titre	Vulnérabilités dans Real Helix RTSP
Date de la première version	27 juin 2006
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

- Real Networks Helix DNA Server 11.0.x ;
- Real Networks Helix DNA Server 10.0.x.

3 Description

Deux vulnérabilités ont été découvertes dans *Real Helix Server*.

La première vulnérabilité, de type débordement de mémoire, concerne le traitement de la donnée `User-Agent` dans l'en-tête. Un utilisateur mal intentionné peut, par le biais d'un en-tête construit de façon malveillante, exécuter du code arbitraire à distance sur le serveur.

La seconde vulnérabilité concerne le traitement des URL.

4 Solution

Appliquer le correctif de l'éditeur (cf. section Documentation).

5 Documentation

- Correctif de l'éditeur :
  https://helix-server.helixcommunity.org/2005/devdocs/builds

Gestion détaillée du document

27 juin 2006 version initiale.