Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 5 avril 2006
N° CERTA-2006-AVI-127-003

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans RealPlayer

Gestion du document

Référence	CERTA-2006-AVI-127-003
Titre	Multiples vulnérabilités dans RealPlayer
Date de la première version	23 mars 2006
Date de la dernière version	5 avril 2006
Source(s)	Bulletin de sécurité du vendeur RealNetworks
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

- RealOne Player v1
- RealOne Player v2
- RealPlayer 8
- RealPlayer 10.x
- RealPlayer Enterprise 1.x
- Helix Player 1.x
- Rhapsody 3

3 Résumé

Plusieurs vulnérabilités présentes dans des produits de RealNetworks permettent à un utilisateur malveillant de lancer une attaque par débordement de tampon et donc d'exécuter du code arbitraire sur la machine de l'utilisateur.

4 Description

Plusieurs vulnérabilités existent dans des produits multimédia RealNetworks, incluant RealPlayer, RealOne, Helix et Rhapsody. Elles peuvent être utilisées par une personne malveillante pour exécuter du code arbitraire sur la machine de l'utilisateur. Nous listons ci-dessous un rapide détail de trois d'entre elles :

- Une erreur dans la manipulation des pages internet peut être utilisée par une personne malveillante pour effectuer un débordement de tampon et exécuter du code arbitraire.
- Une erreur dans l'appel à la fonction `CreateProcess()` permet à un utilisateur local malveillant d'exécuter des programmes placés dans le même répertoire que celui d'un exécutable de RealNetworks.
- Une erreur dans la manipulation de fichiers Flash Media `SWF` permet à un utilisateur malveillant d'effectuer un débordement de tampon et d'exécuter du code arbitraire à distance.

5 Solution

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

6 Documentation

- Bulletin de sécurité de l'éditeur RealNetworks :
  http://service.real.com/realplayer/security
- Bulletin de sécurité RedHat RHSA-2006:0257 du 23 mars 2006 :
  http://rhn.redhat.com/errata/RHSA-2006-0257.html
- Bulletin de sécurité SUSE SUSE-SA:2006:018 du 23 mars 2006 :
  http://www.novell.com/linux/security/advisories/2006_18_realplayer.html
- Bulletin de sécurité Gentoo GLSA 200603-24 du 26 mars 2006 :
  http://www.gentoo.org/security/en/glsa/glsa-200603-24.xml
- Bulletin de sécurité FreeBSD du 4 avril 2006 :
  http://www.vuxml.org/freebsd/pkg-linux-realplayer.html
- Référence CVE CAN-2005-2922 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2922
- Référence CVE CAN-2005-2936 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2936
- Référence CVE CAN-2006-0323 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2922

Gestion détaillée du document

23 mars 2006 version initiale.
5 avril 2006 ajout de la référence au bulletin de sécurité FreeBSD.