Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 11 mars 2005
N° CERTA-2005-AVI-099-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans RealOne Player

Gestion du document

Référence	CERTA-2005-AVI-099-002
Titre	Vulnérabilités dans RealOne Player
Date de la première version	03 mars 2005
Date de la dernière version	11 mars 2005
Source(s)	Bulletin de sécurité de 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 ;
- déni de service.

2 Systèmes affectés

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

3 Résumé

Deux vulnérabilités présentes sur les produits RealNetworks peuvent être exploitées par un utilisateur mal intentionné pour compromettre un système.

4 Description

Plusieurs débordements de mémoire sont présents dans le traitement des fichiers `WAV` (`Windows Audio Video`) et `SMIL` (`Synchronised Multimedia Integration Language`). Ces deux vulnérabilités permettent à un utilisateur mal intentionné, via des fichiers malicieusement construits, de réaliser un déni de service ou d'exécuter du code arbitraire sur le système ayant le service vulnérable.

5 Solution

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

6 Documentation

- Site Internet de RealNetworks :
  http://www.real.com
- Bulletin de sécurité de RealNetworks du 24 février 2005 :
  http://service.real.com/help/faq/security/050224_player/EN/
- Bulletin de sécurité iDEFENSE du 01 mars 2005 :
  http://www.idefense.com/application/poi/display?id=209
- Bulletin de sécurité RedHat RHSA-2005:265 du 03 mars 2005 :
  http://rhn.redhat.com/errata/RHSA-2005-265.html
- Bulletin de sécurité RedHat RHSA-2005:271 du 03 mars 2005 :
  http://rhn.redhat.com/errata/RHSA-2005-271.html
- Bulletin de sécurité SUSE SUSE-SA:2005:014 du 09 mars 2005 :
  http://www.novell.com/linux/security/advisories/2005_14_realplayer.html
- Référence CVE CAN-2005-0455 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0455
- Référence CVE CAN-2005-0611 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0611

Gestion détaillée du document

03 mars 2005 version initiale.

04 mars 2005 ajout des références aux bulletins de sécurité RedHat RHSA-2005:265 et RHSA-2005:271.

11 mars 2005 ajout de la référence CVE CAN-2005-0611 et des bulletins de sécurité iDEFENSE et SUSE SUSE-SA:2005:014.