Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 26 octobre 2007
N° CERTA-2007-AVI-457

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans RealPlayer

Gestion du document

Référence	CERTA-2007-AVI-457
Titre	Multiples vulnérabilités dans RealPlayer
Date de la première version	26 octobre 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité de RealNetworks du 25 octobre 2007
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

- RealPlayer 10.5 (6.0.12.1040 - 6.0.12.1578, 6.0.12.1698, 6.0.12.1741) sur Microsoft Windows ;
- RealPlayer 10 sur Microsoft Windows ;
- RealOne Player v2 sur Microsoft Windows ;
- RealOne Player v1 sur Microsoft Windows ;
- RealPlayer 8 sur Microsoft Windows ;
- RealPlayer Enterprise sur Microsoft Windows ;
- Realplayer 10.1 (10.0.0.305 - 10.0.0.331, 10.0.0.352, 10.0.0.396 - 10.0.0.412, 10.0.0.481) sur MacOS ;
- RealOne Player sur MacOs ;
- RealPlayer 10 (10.0.5 - 10.0.8) sur Linux ;
- Helix Player (10.0.5 - 10.0.8) sur Linux.

3 Résumé

De multiples vulnérabilités permettant à une personne malintentionnée d'exécuter du code arbitraire à distance ont été identifiées dans `RealPlayer`.

4 Description

Cinq vulnérabilités ont été identifiées dans le lecteur multimédia `RealPlayer`. Elles sont dues à des débordements de mémoire qu'une personne malintentionnée distante peut exploiter en incitant l'utilisateur à ouvrir un fichier au format `mp3`, `rm`, `SMIL`, `swf`, `ram` ou `pls` spécialement construit.

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 RealNetworks du 25 octobre 2007 :
  http://service.real.com/main.html
- Référence CVE CVE-2007-2263 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2263
- Référence CVE CVE-2007-2264 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2264
- Référence CVE CVE-2007-3410 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3410
- Référence CVE CVE-2007-4599 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4599
- Référence CVE CVE-2007-5080 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5080
- Référence CVE CVE-2007-5081 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5081

Gestion détaillée du document

26 octobre 2007 version initiale.