



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 06 juillet 2005  
N° CERTA-2005-AVI-230-002

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités des lecteurs RealPlayer

---

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-2005-AVI-230>

---

### Gestion du document

Référence	CERTA-2005-AVI-230-002
Titre	Multiples vulnérabilités des lecteurs RealPlayer
Date de la première version	24 juin 2005
Date de la dernière version	06 juillet 2005
Source(s)	Bulletin de sécurité 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

- Plate-forme Windows :
  - RealPlayer 10.5 (6.0.12.1040-1069);
  - RealPlayer 10;
  - RealOne Player v1;
  - RealOne Player v2;
  - RealPlayer 8;
  - RealPlayer Enterprise 1.x.
- Plate-forme Linux :
  - RealPlayer 10 (10.0.0 -4);
  - Helix Player (10.0.0 -4).
- Plate-forme Mac :
  - RealPlayer 10 (10.0.0.305 -331);
  - Mac RealOne Player;

### 3 Description

Deux vulnérabilités de type débordement de mémoire sont présentes dans le traitement des fichiers `RealMedia` utilisant `RealText` et des fichiers `AVI`.

En incitant un utilisateur à visualiser un de ces fichiers malicieusement construits, il est possible d'exploiter ces vulnérabilités afin d'exécuter du code arbitraire sur le système utilisant le lecteur `RealPlayer`.

Deux autres vulnérabilités affectent les plate-formes Windows :

- par le biais d'un fichier `MP3` malicieusement constitué il est possible d'écraser des fichiers arbitraires sur un système vulnérable ;
- certains paramètres d'Internet Explorer permettent la création et le référencement d'un fichier `HTML` local.

### 4 Solution

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

### 5 Documentation

- Site Internet de RealNetworks :  
<http://www.real.com>
- Bulletin de sécurité de RealNetworks du 23 juin 2005 :  
[http://service.real.com/help/faq/security/050623\\_player/](http://service.real.com/help/faq/security/050623_player/)
- Bulletin de sécurité iDEFENSE id=250 06.23.05 :  
<http://www.iddefense.com/application/poi/display?id=250&type=vulnerabilities>
- Bulletin de sécurité SUSE SUSE-SA:2005:037 du 27 juin 2005 :  
[http://www.novell.com/linux/security/advisories/2005\\_37\\_real\\_player.html](http://www.novell.com/linux/security/advisories/2005_37_real_player.html)
- Mise à jour de sécurité Fedora Core 3 pour HelixPlayer du 24 juin 2005 :  
<http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/>
- Mise à jour de sécurité Fedora Core 4 pour HelixPlayer du 24 juin 2005 :  
<http://download.fedora.redhat.com/pub/fedora/linux/core/updates/4/>
- Bulletin de sécurité Red Hat RHSA-2005:517 du 23 juin 2005 :  
<http://rhn.redhat.com/errata/RHSA-2005:517.html>
- Bulletin de sécurité Red Hat RHSA-2005:523 du 23 juin 2005 :  
<http://rhn.redhat.com/errata/RHSA-2005:523.html>
- Bulletin de sécurité FreeBSD du 24 juin 2005 pour linux-realplayer :  
<http://www.vuxml.org/freebsd/pkg-linux-realplayer.html>
- Bulletin de sécurité Gentoo GLSA 200507-04 du 06 juillet 2005 :  
<http://www.gentoo.org/security/en/glsa/glsa-200507-04.xml>
- Référence CVE CAN-2005-1277 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1277>
- Référence CVE CAN-2005-1766 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1766>

### Gestion détaillée du document

**24 juin 2005** version initiale.

**28 juin 2005** ajout références aux bulletins de SuSE, Red Hat, Fedora et FreeBSD. Ajout références CVE.

**06 juillet 2005** ajout des références aux bulletins de sécurité iDEFENSE et Gentoo.