



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 09 février 2004  
N° CERTA-2004-AVI-024

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités de RealOne Player

---

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-2004-AVI-024>

---

### Gestion du document

Référence	CERTA-2004-AVI-024
Titre	Vulnérabilités de RealOne Player
Date de la première version	09 février 2004
Date de la dernière version	–
Source(s)	Avis de sécurité NGSSoftware #NISR04022004a
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 ;
- RealOne Player v2 ;
- RealPlayer 10 Beta (anglais uniquement) ;
- RealPlayer 8 (toutes les versions localisées) ;
- RealOne Enterprise Desktop ou RealPlayer Enterprise.

## 3 Résumé

Plusieurs problèmes de sécurité dans RealPlayer permettent à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

## 4 Description

RealPlayer est un lecteur multimédia développé par RealNetworks (real.com). Plusieurs problèmes ont été découverts permettant à un utilisateur mal intentionné de :

- exécuter des scripts JavaScript distants depuis le domaine de l'URL ouverte par un fichier SMIL ou un autre fichier ;
- créer des fichiers medias malicieusement construit afin de télécharger et d'exécuter du code arbitraire.

## 5 Solution

Mettre à jour selon les recommandations de l'éditeur (cf. section Documentation). Site internet de téléchargement de RealPlayer :

<http://forms.real.com/real/player/blackjack.html>

## 6 Documentation

- Site internet de RealNetworks :  
<http://www.real.com>
- Avis de sécurité de RealNetwork du 4 février 2004 :  
[http://service.real.com/help/faq/security/040123\\_player/FR/](http://service.real.com/help/faq/security/040123_player/FR/)
- Avis de sécurité NGSSoftware #NISR04022004a :  
<http://www.ngssoftware.com/advisories/realone.txt>
- Avis de sécurité du CERT/CC VU#473814 :  
<http://www.kb.cert.org/vuls/id/473814>
- Avis de sécurité du CERT/CC VU#473902 :  
<http://www.kb.cert.org/vuls/id/473902>
- Avis de sécurité du CERT/CC VU#514734 :  
<http://www.kb.cert.org/vuls/id/514734>

## Gestion détaillée du document

09 février 2004 version initiale.