



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 04 octobre 2004
N° CERTA-2004-AVI-330

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans 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-2004-AVI-330>

Gestion du document

Référence	CERTA-2004-AVI-330
Titre	Vulnérabilités dans RealPlayer
Date de la première version	04 octobre 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité de RealNetworks du 28 septembre 2004
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 ;
- atteinte à l'intégrité des données.

2 Systèmes affectés

- Pour Windows :
 - RealPlayer 10.5 (versions 6.0.12.1040 et antérieures) ;
 - RealPlayer 10 ;
 - RealPlayer 8 ;
 - RealOne Player V1 et V2.
- Pour Mac :
 - RealPlayer 10 Beta ;
 - RealOne Player.
- Pour Linux :
 - Linux RealPlayer 10 ;
 - Helix Player.

3 Résumé

Trois vulnérabilités affectant divers lecteurs RealPlayer permettent l'exécution de code arbitraire à distance ou la suppression de fichiers.

4 Description

Trois vulnérabilités affectent divers lecteurs RealPlayer :

- Une vulnérabilité permet d'exécuter du code arbitraire via un fichier avec l'extension `.rm` malicieusement constitué ;
- une vulnérabilité permet l'exécution de code arbitraire via une page web malicieusement constituée ;
- une vulnérabilité permet la suppression de fichiers dans un chemin connu via une page web et un fichier media malicieusement constitués.

5 Solution

Mettre à jour le lecteur RealPlayer comme indiqué dans le bulletin de sécurité de RealNetworks (voir Documentation).

6 Documentation

Bulletin de sécurité de RealNetworks du 28 septembre 2004 :
http://www.service.real.com/help/faq/security/040928_player/FR

Gestion détaillée du document

04 octobre 2004 version initiale.