



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 juin 2004
N° CERTA-2004-AVI-194

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de 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-194>

Gestion du document

Référence	CERTA-2004-AVI-194
Titre	Multiples vulnérabilités de RealPlayer
Date de la première version	11 juin 2004
Date de la dernière version	-
Source(s)	Avis de sécurité de Real Networks du 10 juin 2004 Avis de sécurité d'iDefense Avis de sécurité d'eEye
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 ;
- RealPlayer 8 ;
- RealPlayer Enterprise.

3 Description

Deux vulnérabilités de type débordement de mémoire sont présentes dans le logiciel Real Player :

- une mauvaise gestion des URL contenant un grand nombre de caractères " . " ;

- une faille dans le composant `embed3260.dll` à la création d'un message d'erreur lors de la réception d'un fichier invalide.

Par le biais d'un site habilement constitué, un individu mal intentionné peut forcer l'exécution de code arbitraire à distance sur le poste d'un utilisateur employant une version vulnérable de Real Player.

4 Solution

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

5 Documentation

- Bulletin de sécurité de Real Networks du 10 juin 2004 :
http://service.real.com/help/faq/security/040610_player/EN
- Avis de sécurité 06.10.04 d'iDefense :
[http://www.idefense.com/application/poi/display?id=109&type=vulnerabilities"](http://www.idefense.com/application/poi/display?id=109&type=vulnerabilities)
- Avis de sécurité AD20040610 d'eEye :
<http://www.eeye.com/html/research/advisories/AD20040610.html>

Gestion détaillée du document

11 juin 2004 version initiale.