

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités du lecteur 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-455>

Gestion du document

Référence	CERTA-2005-AVI-455
Titre	Multiples vulnérabilités du lecteur RealPlayer
Date de la première version	15 novembre 2005
Date de la dernière version	–
Source(s)	Bulletins de sécurité de RealNetworks du 10 novembre 2005
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 (6.0.2.1040-1235) ;
- RealPlayer 10 ;
- RealOne Player v2 ;
- RealOne Player v1 ;
- RealPlayer 8 ;
- RealPlayer Enterprise 1.1, 1.2, 1.5, 1.6 et 1.7 ;
- Mac RealPlayer 10 (10.0.0.305 - 331) ;
- RealPlayer 10 (10.0.0 - 5) ;
- Helix Player (10.0.0 - 5).

3 Résumé

Trois vulnérabilités découvertes dans le lecteur RealPlayer permettent l'exécution de code arbitraire à distance.

4 Description

Deux vulnérabilités de type débordement de mémoire ont été découvertes dans le traitement des fichiers au format .rjs (fichiers « skin »). Une de ces deux vulnérabilités se trouve dans la bibliothèque de compression/décompression DUNZIP32.DLL. Un utilisateur mal intentionné peut, par le biais d'un fichier au format .rjs malicieusement constitué, exécuter du code arbitraire à distance.

Une vulnérabilité dans le traitement des fichiers au format .rm (fichiers RealMedia) a été découverte. Un utilisateur mal intentionné peut, par le biais d'un fichier au format .rm malicieusement constitué, exécuter du code arbitraire à distance.

5 Solution

Appliquer les mises à jour de l'éditeur (voir Documentation).

6 Documentation

- Bulletins de sécurité RealNetworks du 10 novembre 2005 :
http://service.real.com/help/faq/security/051110_player/FR/
<http://service.real.com/help/faq/security/security111005.html>

Gestion détaillée du document

15 novembre 2005 version initiale.