

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité 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-151>

Gestion du document

Référence	CERTA-2005-AVI-151-001
Titre	Vulnérabilité des lecteurs RealPlayer
Date de la première version	21 avril 2005
Date de la dernière version	02 mai 2005
Source(s)	Bulletin de sécurité de RealNetworks Bulletin de sécurité de SuSE
Pièce(s) jointe(s)	Aucune

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

1 Systèmes affectés

- Helix Player (10.0.0 -3);
- RealPlayer 10 (10.0.0 -3) pour Linux;
- RealPlayer 10.5 (6.0.12.1040-1059) pour Windows;
- RealPlayer 10 (10.0.0.305 -311) pour Mac;
- RealOne Player v1 ;
- RealOne Player v2 ;
- RealPlayer 8 ;
- RealPlayer Enterprise 1.x.

2 Description

Une vulnérabilité de type débordement de mémoire est présente dans le traitement des fichiers .RAM (Real Audio Media).

Au moyen d'un fichier .RAM malicieusement construit, un utilisateur mal intentionné peut exploiter cette vulnérabilité afin d'exécuter du code arbitraire sur le système vulnérable.

3 Solution

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

4 Documentation

- Site Internet de RealNetworks :
<http://www.real.com>
- Bulletin de sécurité de RealNetworks du 19 avril 2005 :
http://service.real.com/help/faq/security/050419_player/
- Bulletin de sécurité SUSE SUSE-SA:2005:026 du 20 avril 2005 :
http://www.novell.com/linux/security/advisories/2005_26_realplayer.html
- Mise à jour de sécurité Fedora Core 3 pour HelixPlayer du 19 avril 2005 :
<http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/>
- Bulletin de sécurité Red Hat RHSA-2005:363 du 20 avril 2005 :
<http://rhn.redhat.com/errata/RHSA-2005:363.html>
- Bulletin de sécurité Red Hat RHSA-2005:392 du 20 avril 2005 :
<http://rhn.redhat.com/errata/RHSA-2005:392.html>
- Bulletin de sécurité Red Hat RHSA-2005:394 du 20 avril 2005 :
<http://rhn.redhat.com/errata/RHSA-2005:394.html>
- Bulletin de sécurité Gentoo GLSA 200504-21 du 22 avril 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200504-21.xml>
- Référence CVE CAN-2005-0755 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0755>

Gestion détaillée du document

21 avril 2005 version initiale.

02 mai 2005 ajout référence au bulletin de sécurité Gentoo. Ajout référence CVE.