



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 juillet 2010
N° CERTA-2010-AVI-023-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Realplayer et Helix 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-2010-AVI-023>

Gestion du document

Référence	CERTA-2010-AVI-023-002
Titre	Multiples vulnérabilités dans Realplayer et Helix Player
Date de la première version	21 janvier 2010
Date de la dernière version	15 juillet 2010
Source(s)	Mise à jour de sécurité RealNetworks du 19 janvier 2010
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 ;
- déni de service à distance.

2 Systèmes affectés

Les versions suivantes pour Microsoft Windows sont affectées :

- RealPlayer SP 1.0.0 et 1.0.1 ;
- RealPlayer 11.x ;
- RealPlayer 10.x ;
- RealPlayer Enterprise.

Les versions suivantes pour Mac OS sont affectées :

- Mac RealPlayer 11.x ;
- Mac RealPlayer 10.x.

Les versions suivantes pour GNU/Linux sont affectées :

- GNU/Linux RealPlayer 11.x ;

- GNU/Linux RealPlayer 10.x ;
- Helix RealPlayer 11.x ;
- Helix RealPlayer 10.x.

3 Résumé

Plusieurs vulnérabilités dans les produits RealNetworks permettent à un utilisateur distant malintentionné de provoquer un déni de service ou d'exécuter du code arbitraire.

4 Description

Onze vulnérabilités, de type débordement de mémoire, ont été découvertes dans les produits RealPlayer et Helix Player. Ces vulnérabilités peuvent être exploitées par une personne distante malveillante afin de provoquer un déni de service ou encore d'exécuter du code arbitraire.

5 Solution

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

6 Documentation

- Mise à jour de sécurité RealNetworks du 19 janvier 2010 :
http://service.real.com/realplayer/security/01192010_player/en/
http://service.real.com/realplayer/security/01192010_player/fr/
- Bulletin de sécurité Sun Solaris du 13 juillet 2010 :
http://blogs.sun.com/security/entry/cve_2009_4247_buffer_overflow
- Référence CVE CVE-2009-0375 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0375>
- Référence CVE CVE-2009-0376 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0376>
- Référence CVE CVE-2009-4241 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4241>
- Référence CVE CVE-2009-4242 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4242>
- Référence CVE CVE-2009-4243 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4243>
- Référence CVE CVE-2009-4244 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4244>
- Référence CVE CVE-2009-4245 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4245>
- Référence CVE CVE-2009-4246 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4246>
- Référence CVE CVE-2009-4247 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4247>
- Référence CVE CVE-2009-4248 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4248>
- Référence CVE CVE-2009-4257 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4257>

Gestion détaillée du document

21 janvier 2010 version initiale ;

16 février 2010 correction du lien vers la mise à jour de sécurité ;

15 juillet 2010 ajout de la référence au bulletin de sécurité Sun Solaris.