

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples 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-2010-AVI-411>

Gestion du document

Référence	CERTA-2010-AVI-411
Titre	Multiples vulnérabilités dans RealPlayer
Date de la première version	30 août 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité RealNetworks du 26 août 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 ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- RealPlayer versions antérieures à la SP 1.1.5 ;
- Mac RealPlayer versions antérieures à la 12.0.0.1444 ;
- RealPlayer Enterprise versions antérieures à la 2.1.2 ;
- Linux RealPlayer versions antérieures à la 11.0 ;
- Helix RealPlayer versions antérieures à la 11.0.

3 Résumé

Plusieurs vulnérabilités dans RealPlayer permettent à une personne malintentionnée de porter atteinte à la confidentialité des données ou d'exécuter du code arbitraire à distance.

4 Description

De multiples vulnérabilités dans `RealPlayer` ont été découvertes. Elles permettent à une personne malintentionnée de porter atteinte à la confidentialité de certaines données et d'exécuter du code arbitraire à distance notamment via des fichiers *FLV* ou *QCP*.

5 Solution

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

6 Documentation

- Bulletin de sécurité RealNetworks du 26 août 2010 :
http://service.real.com/realplayer/security/08262010_player/en/
- Référence CVE CVE-2010-0116 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0116>
- Référence CVE CVE-2010-0117 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0117>
- Référence CVE CVE-2010-0120 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0120>
- Référence CVE CVE-2010-2996 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2996>
- Référence CVE CVE-2010-3000 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3000>
- Référence CVE CVE-2010-3001 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3001>
- Référence CVE CVE-2010-3002 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3002>

Gestion détaillée du document

30 août 2010 version initiale.