



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 juillet 2008
N° CERTA-2008-AVI-378

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-2008-AVI-378>

Gestion du document

Référence	CERTA-2008-AVI-378
Titre	Multiples vulnérabilités dans RealPlayer
Date de la première version	28 juillet 2008
Date de la dernière version	–
Source(s)	Bulletin de mise à jour de RealPlayer du 25 juillet 2008
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

Les versions antérieures aux suivantes sont vulnérables :

- RealPlayer pour Windows 11.0.3 build 6.0.14.806 ;
- RealPlayer pour Windows Vista 10.5 build 6.0.12.1675 ;
- RealPlayer pour Mac 11 ;
- RealPlayer pour Linux 11.

3 Résumé

Plusieurs vulnérabilités affectant RealPlayer sur différentes plateformes ont été corrigées.

4 Description

Quatre vulnérabilités affectant `RealPlayer` ont été corrigées par la dernière mise à jour. Deux concernent l'*ActiveX* associé au lecteur multimédia alors qu'une autre est présente lors de la lecture de fichier *SFW*. La dernière, non documentée, permet un dépassement de mémoire.

5 Solution

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

6 Documentation

- Bulletin de mise à jour de `RealPlayer` du 25 juillet 2008 :
http://service.real.com/realplayer/security/07252008_player/en
- Référence CVE CVE-2007-5400 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5400>
- Référence CVE CVE-2008-1309 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1309>
- Référence CVE CVE-2008-3064 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3064>
- Référence CVE CVE-2008-3066 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3066>

Gestion détaillée du document

28 juillet 2008 version initiale.