README.md

Real Player 'DCP://' URI Remote Arbitrary Code Execution Vulnerability

video demo: https://youtu.be/AMODp3iTnqY

The 'DCP://' URI scheme is an internal protocol used by Real Player to retrieve URLs to display in the Player browser tab. It stands for 'Data Cache Protocol'. It will retrieve files from '%appdata%\real\realplayer'. These files are simple '.ini' files with the following code:

---sample_dcp.ini--- [urls] onlineurl=http://example.com/ offlineurl=file:///c:/example.htm

The 'offlineurl' attribute seems to be ignored, however it´s possible to pass arbitrary URLs, including URLs to local files and unsafe 'Javascript:' URIs.

Example: dcp://custom.ini

This potentially creates an universal cross site scripting condition (uXSS).

Real Player uses Microsoft Internet Explorer functionality and exposes properties and methods through a special mean which is application specific:

The 'external' object and it exposes several custom methods and properties.

It´s not possible to retrieve remote files, but it´s possible to use parent directories (..) to retrieve the files. For that we can use 'external::OpenURLInPlayerBrowser()' method

By combining this issue with a file planting issue with the 'external::RecordClip()' method, we are able to plant valid '.ini' files (although they are extensionless) on a predictable location:

'Videos\RealPlayer Downloads'.

By planting 2 files, and further referencing them via a 'DCP://' URI it´s possible to reference an URL belonging to an arbitrary domain or "security zone" (Windows Security zones) and then inject custom javascript code.

The PoC uses code that causes the prompt for unsafe ActiveX controls to be "defeated" and run MSHTA pointing to the second file that has code to run 'cmd.exe'. It could contain eg. an embedded EXE

To reproduce this issue, all you need is to edit the files and replace '%server%' with the actual server host name or IP. Also replace '%username%' with the target´s actual Windows user name on the files 'dcp1.txt' and 'rp_dcp.htm'

Note: The Windows username can be obtained via requests to an SMB server or WebDAV server.

Affected versions: 16.0.3.51, Cloud 17.0.9.17, v.20.0.7.309 on any Windows version (XP up to 11)

Releases

No releases published

Packages

No packages published