Edubr2020 / **RealPlayer_G2_RCE** Public

☆ 4 stars 1 fork

☆ Star ▾ Notifications

main ▾ Go to file

Edubr2020 Update README.md ... on May 31 4

View code

README.md

Real Player v.20.0.8.310 G2 Control 'DoGoToURL()' Remote Code Execution Vulnerability

Video demo: https://www.youtube.com/watch?v=9c9Q4VZQOUk

Real Player G2 Control component contains a remote code execution vulnerability because it allows 'javascript:' URIs to be passed as the argument, which is usually not safe because in some scenarios could allow injection of script code in arbitrary domains (Universal Cross Site Scripting - uXSS) which can potentially be used to eg. steal cookies among other things. By setting the 'URL' parameter to 'javascript:' URI and the 'target' parameter to an 'iframe' html element, it´s possible to cause javascript code to run in the context of a local error page displayed after using the very same Control to navigate to an invalid URI such as 'mhtml:http://%SERVER%/frame.htm': when an 'mhtml:' URI is invoked by MS IE rendering engine, it expects an MHTML file with an extension whose MIME type is set to "message/rfc822", which is the case for '.mht' files; '.htm' files have its MIME set to 'text/html' and thus IE will cancel loading the document and display a local error page (navigation cancelled). The local error page address is 'res://ieframe.dll/navcancl.htm' which belongs to the 'My computer' security zone of IE / Windows which allows reading of arbitrary local files and also arbitrary code execution by design. Prohibiting the 'javascript:' URI in the control mitigates the issue.

The PoC uses the 'SYSMON' ActiveX control to plant an HTA file to the user´s startup folder, which will be executed on next logon or boot. an HTA file can contain code to eg. download or extract an embedded EXE file and run it. The PoC assumes Real Player has its current working directory set to a subdirectory of the user´s home directory. Upon downloading files using eg. web browsers, they will be downloaded to the user´s 'Downloads' folder by default, so we don´t need to retrieve the Windows user name to be able to plant the HTA file in the startup folder. This is just for convenience purposes as it´s possible to retrieve this info through a variety of ways, including the MS Web Browser ActiveX.

Vulnerability can be exploited by opening a Real Player playlist file such as RAM files.

To reproduce the issue, do the following:

a) Setup a web server b) on the web server root directory, extract the "RP_G2" folder to it. c) open the just extracted "RP_G2" folder and then open the following files in a text editor: "poc.htm", "sm_rpx.js", "start.ram". Just replace every occurance of the string %SERVER% with the actual web server´s IP address (on each of the files) d) make sure the web server is accessible and all involved files too. on MS IIS web server you may need to add a new extension and associate it with a MIME type, so do it to associate the .RAM extension with the MIME "audio/x-pn-realaudio". e) on the client side (victim), open the web browser and download the "start.ram" file (or can be accessed eg. using a URL protocol such as 'rtsp:') and open it. You should see an HTA file being planted in the user´s startup folder after a few seconds.

Note: to open startup folder do this: open the "Run" menu and then type:

shell:Startup

hit enter and voila.

Successfully tested on Real Player v.20.0.8.310 (and below versions going back several years, like 2014 or so) running on Windows XP SP3, Vista, 7, 8.1, 10, 11 all fully patched with its most recent patches. (eg. Windows XP most recent update was on April, 2014... Win 7 on January 2020, and so on)

Releases

No releases published

Packages

No packages published