README.md

Real Player 'external::Import()' Arbitrary file download, Directory Traversal Vulnerabilities leads to Remote Code Execution

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

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.

The 'Import()' method is handled in unsafe way regarding the 'Copy to My Music' parameter, which allows for arbitrary file types downloading which could be unsafe as only audio/image/video types should be allowed to download to the user´s disk. Additionally it does not properly sanitize file paths allowing planting of arbitrary files on arbitrary locations. Even though it displays an error because it cannot render the downloaded file, the file remains until the user closes the dialog box. Additionally when opening new windows, Real Player looks for an old, obsolete IE library (shdoclc.dll), which can also be abused to run code automatically without needing to wait until reboot (true when file is planted in 'startup' folder).

The attacker needs to host the files to be copied/downloaded in an SMB or WebDav share. The directory 'appdata' must be placed in the share´s root.

Also a DOS condition in 'external.PreloadURL()' helps so that the files are not deleted by Real Player

The PoC will drop 'shdoclc.dll' (has simple code to run 'cmd.exe' at 'DllMain()' for demonstration purposes) to the user´s 'windowsapps' folder and 'write.exe' to 'startup' folder, so it works universally (any Windows version from at least XP up to 11)

tested on RP ver. 16.00.282, 16.0.3.51, Cloud 17.0.9.17, v.20.0.7.309

Releases

No releases published

Packages

No packages published