CastSrv.exe Elevation of Privilege Vulnerability

## surroundings

Microsoft Windows 10.0.18363.592 64-bits

## Vulnerability description

Since the com interactive interface CCastServerControl::GetEnableControl does not handle symbolic links, it is possible to create arbitrary controllable directories under another user

## **Vulnerability root cause**

CastSrv.exe supports some interactive interfaces, the following is the information of the vulnerable interface

clsid: f8842f8e-dafe-4b37-9d38-4e0714a61149

uuid: 7733f245-f909-4be2-918f-bddecbcd07cc

clsid name: CastServerInteractiveUser

interfaces name: ICastServerControl

Vulnerable method name: ICastServerControl::GetEnableControl

Due to the interactive nature of this interface, if we instantiate the interface with another logged in user session number, CastSrv.exe will run in the context of another logged in user

ICastServerControl::GetEnableControl supports a parameter that takes a fixed pointer as a parameter

Once we pass in a pointer, CastSrv.exe will create the \AppData\Local\\_\_SHARED\PlayToReceiver directory in the current user directory (the user represented by the CastSrv.exe session) and create some image files

The problem here is:

1. \_\_SHARED is and PlayToReceiver will be set to a dacl that can fully control all users

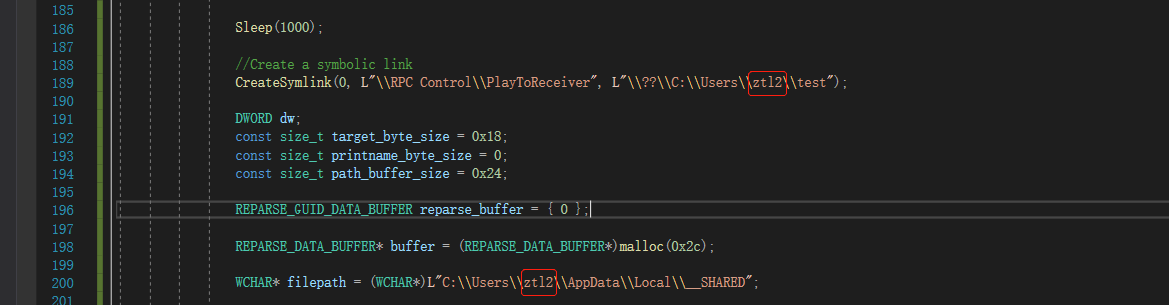
2. The symbolic link is not judged when creating \_\_SHARED and PlayToReceiver

Obviously, we can use these two points to create any fully controllable directory under another user

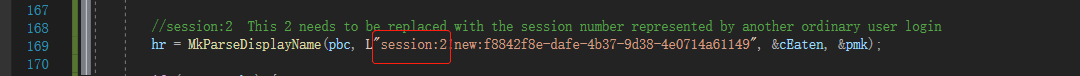
## POC

Before running the poc, first you probably need to modify my code,

There are two places in the red box in the picture below, you need to change the two places ztl2 to another username



Finally you may need to change the session number to another session number where the logged in user is



Below I will explain what the poc does

1. Instantiate ICastServerControl under another user session

2. Call ICastServerControl::GetEnableControl once to trigger the creation of C:\Users\another login username\AppData\Local\\_\_SHARED\PlayToReceiver

3. Set PlayToReceiver as a symlink to C:\Users\another login username\test, Empty the files under C:\Users\another login username\AppData\Local\\_\_SHARED and set it as the mount point

4. Finally call ICastServerControl::GetEnableControl once, CastSrv.exe will follow the symbolic link to create the target file

Expected print result

