CoreShellExtFramework.dll Elevation of Privilege Vulnerability

**environment**

Microsoft Windows Version 10.0.19042.928 64-bits

**Vulnerability description**

There are access control vulnerabilities in CoreShellExtFramework.dll!CoreShellComServerRegistrar::OpenProcess

Attackers can manipulate the handle of the medium process as a Low privilege.

**Causes of Vulnerability**

The vulnerability of CoreShellComServerRegistrar::OpenProcess is caused by not verifying whether the target process can access or calling DuplicateHandle directly

And we don’t need to pass in the process handle, just pass the process pid, UMgrOpenProcessHandleForAccess will help us open the process

we can control all the parameters of the function

CoreShellComServerRegistrar::OpenProcess(CoreShellComServerRegistrar \*this, unsigned int a2, BOOL a3, unsigned int a4, unsigned int a5, unsigned \_\_int64 \*lpTargetHandle)

{

v10 = GetCurrentProcessId();

v11 = UMgrOpenProcessHandleForAccess(64i64, v10, v9);

v12 = v11;

if ( v11 >= 0 )

{

hTargetProcessHandle = 0i64;

v14 = UMgrOpenProcessHandleForAccess(64i64, a5, v13);

v12 = v14;

if ( v14 >= 0 )

{

v16 = UMgrOpenProcessHandleForAccess(a2, a4, v15);

v12 = v16;

if ( v16 >= 0 )

{

if ( DuplicateHandle(

hSourceProcessHandle,

hSourceHandle,

hTargetProcessHandle,

(LPHANDLE)lpTargetHandle,

0,

a3,

2u) )

**EXP**

Once a process handle with medium privileges is obtained, the remote thread is used to inject the CMD with medium privileges

You need to run the exp under low permissions. After running, you should get a CMD with medium permissions.