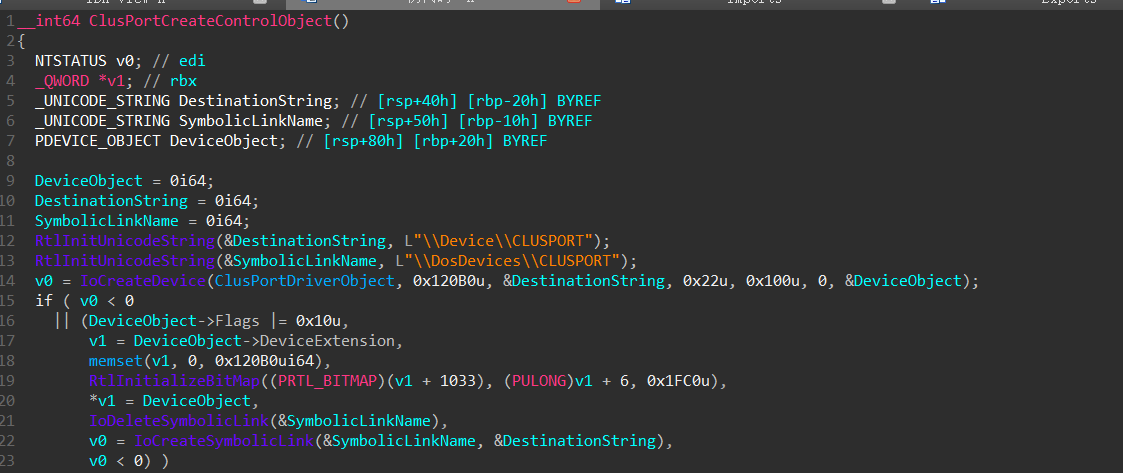
Windows Server 2022 Version 10.0.20348.169 64-bits

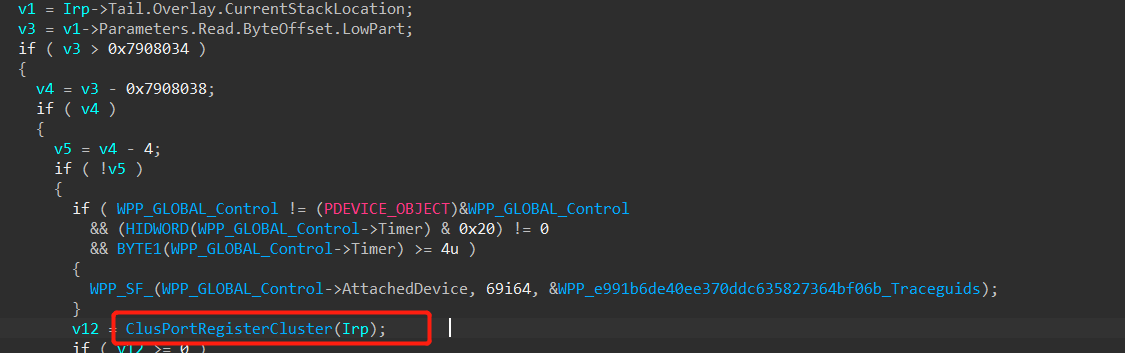
Vulnerability description

Because ClusPort.sys does not correctly verify the user's input buffer, attackers can use this vulnerability to cause computer crashes

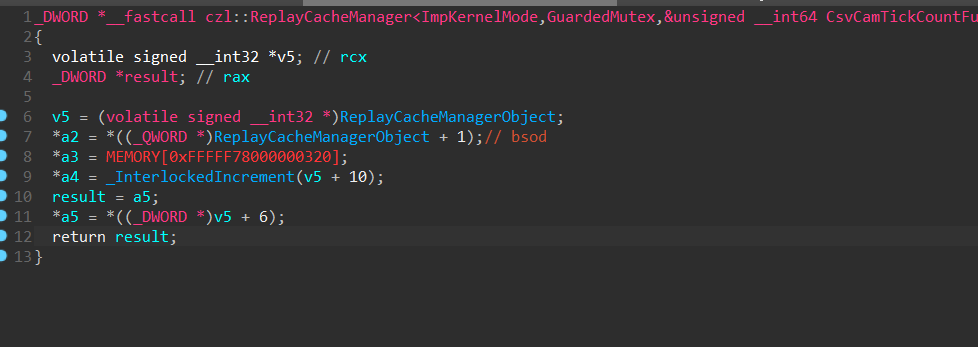
Causes of Vulnerability

ClusPort.sys will create a device link name CLUSPORT, which can be opened and written under the low process permission

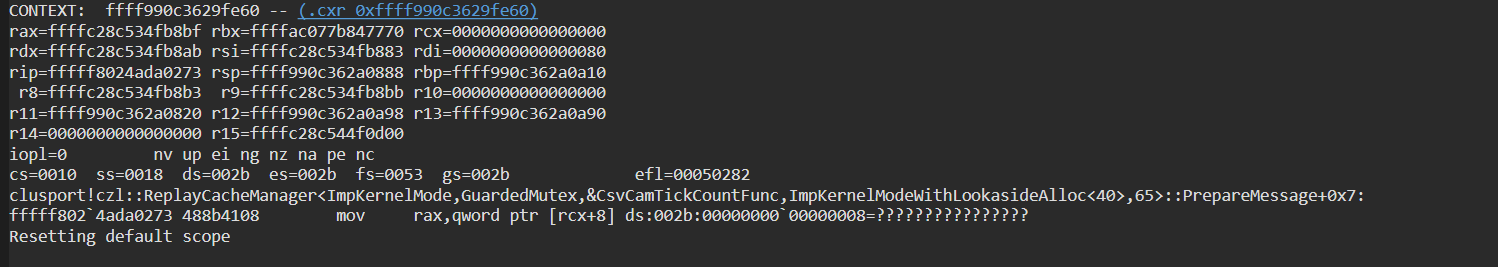


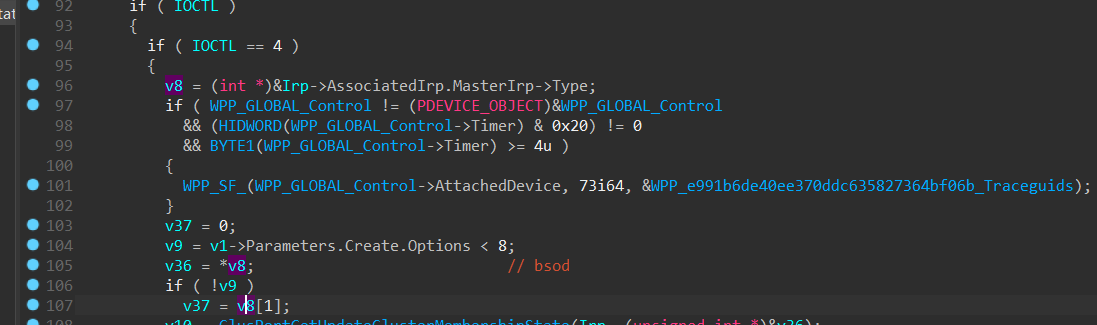


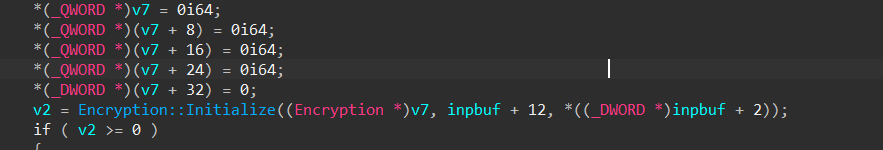
czl::ReplayCacheManager, the problem here is that whether ReplayCacheManagerObject is initialized or not is determined by the user. If the user does not initialize the variable before triggering ClusPortRegisterCluster, the variable will be 0, which will trigger a null pointer dereference vulnerability, and the kernel will access memory at address 0. Cause the computer to crash



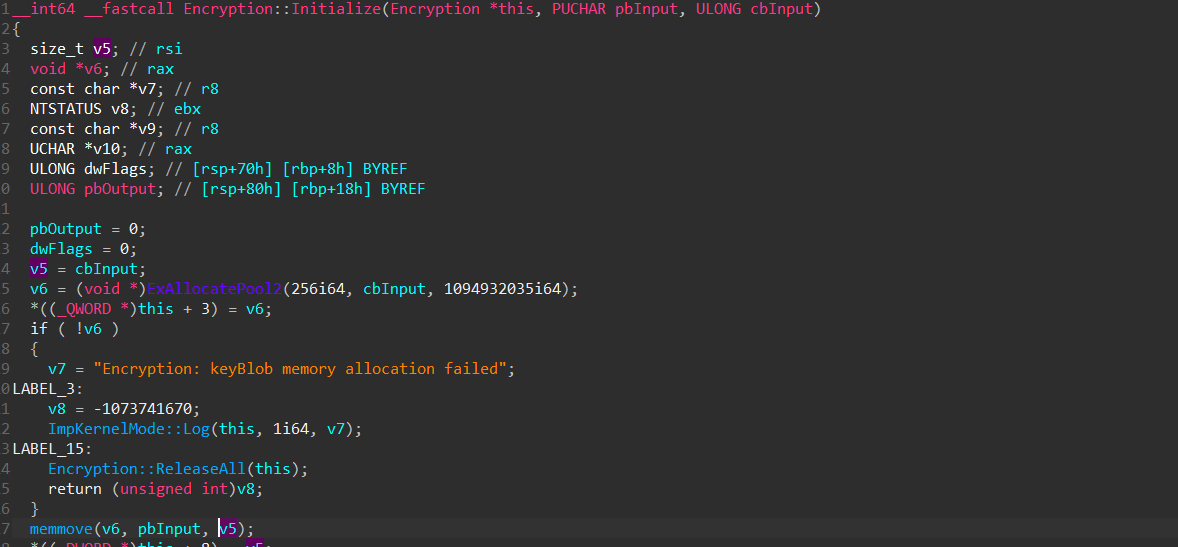
Dump



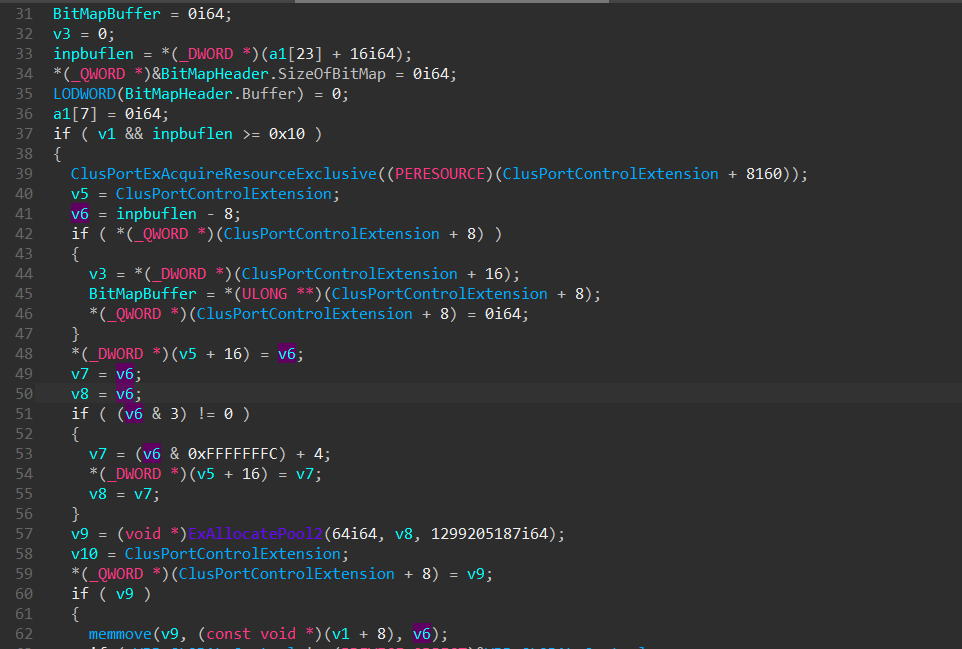
Another vulnerability with null pointer dereference is located in ClusPortControlObjectDeviceControlHandler As shown in the figure below, although inpbuflen is judged here, the first four bytes v8 in inpbuf are referenced before the judgment, which causes a null pointer reference. 

The other two vulnerabilities are ClusPortUpdateMembership and CsvCamSetSecurityInfo. These two are ioctl processing functions. Even if their ioctls are different, their causes of vulnerabilities are very similar. CsvCamSetSecurityInfo will call Encryption::Initialize and pass inpbuf 

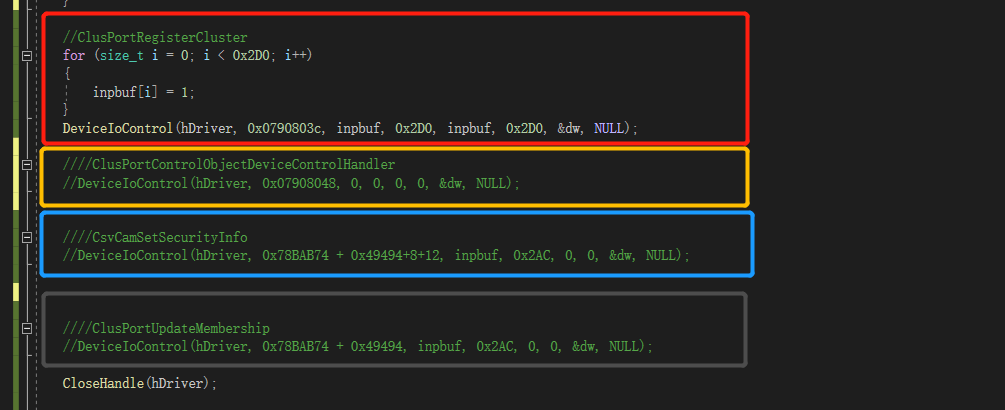
The problem with Encryption::Initialize is that there is no judgment on the length of the memmove cbInput, because the length here is user-controllable, so you can set a length that exceeds the user's inpbuf to trigger the out-of-bounds read vulnerability.



ClusPortUpdateMembership is also the cause of the vulnerability. The length of the memmove is not judged, resulting in out-of-bounds reading



In order to trigger the vulnerability, I made a poc, the poc will open the symbolic link CLUSPORT and then call DeviceIoControl to trigger the vulnerability As shown in the figure below, the code in different borders triggers different vulnerabilities.



You can run poc.exe in the Low process environment, and then check whether the computer crashes If not, you should check whether ClusPort.sys is starting, if not, you should need to install the server function represented by ClusPort.sys

Since I installed as many service components as possible, I regret that I didn’t figure out what functions the file depends on. After the function represented by ClusPort.sys is installed, it will automatically start after booting by default