吴先生，您好:

粤总 and 毓杰，您们好:

如之前沟通，根据已收集的 dump，针对此问题，目前已分析完毕。请您邮件确认此问题分析结果:

Case No：CAS-02812-Q3D7K7

问题描述:
==========
用户反馈，登录华为云桌面，输入完密码电脑蓝屏，希望分析蓝屏原因。

问题分析:
==========

在开启 special pool 的情况下，detect 到外设类 PNP 设备在发起 irp 之后，被华为云桌面执行 complete 的违规操作，导致蓝屏。

正常情况下，操作系统或应用程序在访问外设类 PNP 设备进行 IO 操作时，会根据设备发起的 irp 进行判断，最终传递至需要进行 IO 操作的场景。此案例中，在处理非华为云桌面客户端接收的 IO 操作时，hwusbclient 应在处理 PNP irp 事件中标注 pass down，以使得 irp 继续向下层传递，然而华为云桌面错误标记为 complete，最终导致蓝屏。

具体分析如下:

```
2: kd> !mex.crash
Dump Info
==========================================
Dump Name: MEMORY-huawei1.DMP
Windows 10 Kernel Version 17763 MP (4 procs) Free x64
Product: WinNt, suite: TerminalServer SingleUserTS
Edition build lab: 17763.1.amd64fre.rs5_release.180914-1434
Kernel base = 0xfffff800`3ba0e000 PsLoadedModuleList =
0xfffff800`3be286f0
Debug session time: Tue Aug 18 14:39:36.730 2020 (UTC + 8:00)
System Uptime: 0 days 0:05:38.360
Processor: Intel(R) Core(TM) i5-4300U CPU @ 1.90GHz
Bugcheck: C9 (22E, FFFFF8003E88AD80, FFFFA40F24CAE270, 0)
Kernel Complete Dump File: Full address space is available.


Bugcheck details
```

```
=============================================
DRIVER_VERIFIER_IOMANAGER_VIOLATION (c9)
The IO manager has caught a misbehaving driver.
Arguments:
Arg1: 000000000000022e, The caller has completed a successful IRP_MJ_PNP
instead of passing it down.
Arg2: fffff8003e88ad80, The address in the driver's code where the error
was detected.
Arg3: ffffa40f24cae270, IRP address.
Arg4: 0000000000000000
```

根据 bugcheck 和 call stack，问题是三方 IO 驱动 hwusbclient 在进行 IO 操作时引起的，具体的说明可以参考如下的 link:
https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/bug-check-0xc9--driver-verifier-iomanager-violation

0x22E	Non-fatal error	The caller has completed a successful IRP_MJ_PNP instead of passing i Param 2 - The address in the driver's code where the error was detecte Param 3 - IRP address.

```
Crashing Stack
=============================================
Process                                    Thread                    C
ID             UserTime KernelTime ContextSwitches Wait
Reason           Time State
System (ffffa40ef2f0a440) ffffa40f25282700
4.1e00                    0s         2s.594                    74052
WrYieldExecution     0s Running on CPU 2

Irp List:
       IRP                          File Driver
       ffffa40efcf23010           USBHUB3

# Child-SP                 Return                   Call
Site
                           Source
```

```
0 ffffa18fa3d31b88 fffff8003c33de63
nt!KeBugCheckEx+0x0

  1 ffffa18fa3d31b90 fffff8003c34428f
nt!VerifierBugCheckIfAppropriate+0xdf
  2 ffffa18fa3d31bd0 fffff8003bd1625f
nt!ViErrorFinishReport+0x117

  3 ffffa18fa3d31c30 fffff8003c34e908
nt!ViErrorReport1+0x63

  4 ffffa18fa3d31cd0 fffff8003c343df0
nt!VfPnpVerifyIrpStackUpward+0x158
  5 ffffa18fa3d31d30 fffff8003c33d703
nt!VfMajorVerifyIrpStackUpward+0x74
  6 ffffa18fa3d31d80 fffff8003c332776
nt!IovpCompleteRequest2+0xe3
  7 ffffa18fa3d31df0 fffff8003bb208bd
nt!IovpLocalCompletionRoutine+0x96
  8 ffffa18fa3d31e50 fffff8003c332191
nt!IopfCompleteRequest+0x1cd
  9 ffffa18fa3d31f60 fffff8003bc48d81
nt!IovCompleteRequest+0x1bd
  a ffffa18fa3d32050 fffff8003e88b0fd
nt!IofCompleteRequest+0x1286c1
  b ffffa18fa3d32080 fffff8003bb7e7ca HwUsbClient+0xb0fd
  c ffffa18fa3d32390 fffff8003c331f49
nt!IopfCallDriver+0x56

  d ffffa18fa3d323d0 fffff8003bc46441
nt!IovCallDriver+0x275

  e ffffa18fa3d32410 fffff80acd96d805
nt!IofCallDriver+0x12f0d1

  f (Inline)                 ----------------
Wdf01000!FxIrp::CallDriver+0x23

10 (Inline)                  ----------------
Wdf01000!FxIrp::SendIrpSynchronously+0xa0
```

```
11 ffffa18fa3d32450 fffff80acd96d2b1
Wdf01000!GetStackCapabilities+0x135
12 (Inline)                 ----------------
Wdf01000!FxPkgPdo::PnpQueryCapabilities+0x89
13 ffffa18fa3d324e0 fffff80acd962ef3
Wdf01000!FxPkgPdo::_PnpQueryCapabilities+0xb1
14 ffffa18fa3d325b0 fffff80acd961b72 Wdf01000!FxPkgPnp::Dispatch+0xb3
15 (Inline)                 ----------------
Wdf01000!DispatchWorker+0x9d

16 (Inline)                 ----------------
Wdf01000!FxDevice::Dispatch+0xbb

17 ffffa18fa3d32620 fffff8003e88cf8b
Wdf01000!FxDevice::DispatchWithLock+0x112
18 ffffa18fa3d32680 fffff8003e889642 HwUsbClient+0xcf8b
19 ffffa18fa3d32700 fffff8003e88b085 HwUsbClient+0x9642
1a ffffa18fa3d32780 fffff8003bb7e7ca HwUsbClient+0xb085

This thread is crashing
```

相关的问题组件

```
2: kd> lmvm hwusbclient
Browse full module list
start             end                 module name
fffff800`3e880000 fffff800`3e8a5000   HwUsbClient   (no symbols)
    Loaded symbol image file: HwUsbClient.sys
    Image path: \SystemRoot\System32\drivers\HwUsbClient.sys
    Image name: HwUsbClient.sys
    Browse all global symbols  functions  data
    Timestamp:        Tue May 14 18:02:33 2019 (5CDA9239)
    CheckSum:         0002CA1C
    ImageSize:        00025000
    Translations:     0000.04b0 0000.04e4 0409.04b0
```

下一步动作:

==========

建议联系华为云桌面客户端厂商进行问题排查，谢谢

李琦 Li Qi
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.

服务电话： 4008180055
电子邮箱 Email: liqi@cmgos.com

神州网信 CMIT

发件人: Li Qi <liqi@cmgos.com>
发送时间: 2020 年 8 月 18 日 18:34
收件人: 吴毓杰 <win10sup@sdc.icbc.com.cn>
抄送: Li Qi <liqi@cmgos.com>
主题: [案例号: CAS-02812-Q3D7K7] % |P3|ICBC|登录华为云桌面电脑蓝屏 % 初次响应 CMIT:0001728

吴毓杰 先生/女士，您好!

感谢您联系神州网信技术支持中心。 我是技术支持工程师 李琦 。 很高兴能有机会协助您解决该问题。 您可随时通过邮件回复以及该问题事件号码 CAS-02812-Q3D7K7 与我联系。

如果您有任何其他疑问，请随时与我联系。

此致,

敬礼
