收到，谢谢李工。

发件人：   Li Qi <liqi@cmgos.com>
收件人：   吴毓杰 <win10sup@sdc.icbc.com.cn>, "liyue@sdc.icbc.com.cn" <liyue@sdc.icbc.com.cn>
抄送：   CRM Case Email <casemail@cmgos.com>, Liu Wei <liuwei@cmgos.com>, Li Xin <lixin@cmgos.com>, Qi Feng <qifeng@cmgos.com>, Wang Dan <wangdan@cmgos.com>, Wang Wenlei <wangwl@cmgos.com>
日期：   2020/08/19 17:02
主题：   回复: [案例号: CAS-02813-G5J7Z5] % |P3|ICBC|无线网络环境下拷贝数据设备蓝屏 % 初次响应 CMIT:0001730

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-02813-G5J7Z5

问题描述：
=====================
用户反馈，无线网络环境下拷贝数据设备蓝屏

问题分析：
=====================
问题原因同 TMS 的 vwifimf 问题,由 pTOS 数据异常造成 page fault 引发蓝屏

Dump 分析：
Bugcheck 0x1e， 系统发现了 pagefault 抛出异常

```
KMODE_EXCEPTION_NOT_HANDLED (1e)
This is a very common bugcheck.  Usually the exception address pinpoints
the driver/function that caused the problem.  Always note this address
as well as the link date of the driver/image that contains this address.
Arguments:
Arg1: ffffffff80000003, The exception code that was not handled
Arg2: fffff801404e6235, The address that the exception occurred at
Arg3: ffff840132bde868, Parameter 0 of the exception
Arg4: ffff840132bde0b0, Parameter 1 of the exception

2: kd> .trap 0xffff840132bdfb50
NOTE: The trap frame does not contain all registers.
Some register values may be zeroed or incorrect.
rax=0000003200360035 rbx=0000000000000000 rcx=ffffda8acc2ec2c0
rdx=0000000000000000 rsi=0000000000000000 rdi=0000000000000000
rip=0000003200360035 rsp=ffff840132bdfce8 rbp=0000000000000000
r8=4c46444e02156700  r9=ec770c55eb0493df r10=ffffda8acc232320
r11=0000000000000001 r12=0000000000000000 r13=0000000000000000
```

```
r14=0000000000000000 r15=0000000000000000
iopl=0         nv up ei pl nz na pe nc
00000032`00360035 ??              ???

2: kd> !mex.t
Process                    Thread          CID     UserTime KernelTime
ContextSwitches Wait Reason Time State
System (ffffda8ac4a63200) ffffda8ac6402080
4.d0           0s      8s.828               59916 Executive     0s Running on CPU
2

 # Child-SP          Return          Call
Site                                  Info
 0 ffff840132bdd808 fffff80140745107
nt!KeBugCheckEx+0x0
 1 ffff840132bdd810 fffff801406841b6
nt!KiFatalFilter+0x1f
 2 ffff840132bdd850 fffff8014064554f
nt!KeExpandKernelStackAndCalloutInternal$filt$0+0x16
 3 ffff840132bdd890 fffff80140673b5f
nt!__C_specific_handler+0x9f
 4 ffff840132bdd900 fffff801405cc450
nt!RtlpExecuteHandlerForException+0xf
 5 ffff840132bdd930 fffff801404d9c24
nt!RtlDispatchException+0x430
 6 ffff840132bde080 fffff8014067c9c2
nt!KiDispatchException+0x144
 7 ffff840132bde730 fffff80140676681
nt!KiExceptionDispatch+0xc2
 8 ffff840132bde910 fffff801404e6236
nt!KiBreakpointTrap+0x301                TrapFrame @ ffff840132bde910
 9 ffff840132bdeaa0 fffff801406454eb
nt!KeCheckStackAndTargetAddress+0x46
 a ffff840132bdead0 fffff80140673b5f
nt!__C_specific_handler+0x3b
 b ffff840132bdeb40 fffff801405cc450
nt!RtlpExecuteHandlerForException+0xf
 c ffff840132bdeb70 fffff801404d9c24
nt!RtlDispatchException+0x430
 d ffff840132bdf2c0 fffff8014067c9c2
nt!KiDispatchException+0x144
 e ffff840132bdf970 fffff80140678cae
nt!KiExceptionDispatch+0xc2
 f ffff840132bdfb50 0000003200360035
nt!KiPageFault+0x42e                     TrapFrame @ ffff840132bdfb50
10 ffff840132bdfce8 fffff8013ed59513 0x3200360035
11 ffff840132bdfcf0 fffff8013ed5d66d
nwifi!Dot11SendCompletion+0x4b
12 ffff840132bdfd30 fffff80143b766a3
nwifi!Pt6SendComplete+0x1d
13 ffff840132bdfd60 fffff80143b784ce
ndis!ndisCallSendCompleteHandler+0x33
14 ffff840132bdfda0 fffff80140597a78
ndis!ndisDataPathExpandStackCallback+0x3e
```

内存空间 0x00000032`00360035 存放的是数据体 **pTOS 的参数 pRoutine**，pTOS 是由三方迷你网卡过滤驱动（mini-port filter driver）vwifimf.sys 维护的。

```
2: kd> !mex.ddt -n pTOS

dt -n pTOS  () Recursive: [ -r1 -r2 -r ] Verbose dx Normal dt
========================================================================
====
Local var @ rbx Type DOT11_COMPLETION_STACK_ENTRY*
   +0x000 pRoutine                     : 0x00000032`00360035 Void    [ !ndao dps
dc !handle ln ? ]
   +0x008 pCtxt                        : 0x4c46444e`02156700 Void    [ !ndao dps
dc !handle ln ? ]
   +0x010 pCtxt2                       : 0xec770c55`eb0493df Void    [ !ndao dps
dc !handle ln ? ]
```

下一步动作:
======================
建议联系 TMS 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

发件人: Li Qi <liqi@cmgos.com>
发送时间: 2020 年 8 月 18 日 18:36
收件人: 吴毓杰 <win10sup@sdc.icbc.com.cn>
抄送: Li Qi <liqi@cmgos.com>
主题: [案例号: CAS-02813-G5J7Z5]％ |P3|ICBC|无线网络环境下拷贝数据设备蓝屏 ％初次响应
CMIT:0001730

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-02813-G5J7Z5 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

以上内容是一封有关向神州网信技术有限公司提交技术支持事件的邮件。

如果您希望本次回复能够被自动加入技术支持事件中**, 您可以**选择"**全部回复**"。