吴先生 您好:

感谢您的电话接听。

根据刚才的沟通情况，我将暂时归档此案例。

工单的归档并不会影响我们为您提供技术支持服务，如您有其他问题，您可以致电技术支持热线 4008180055。

案例总结：

问题定义：

工行云南行一体机安装 11 月补丁，调整 TMS 分组后，出现蓝屏问题。

问题总结：

dump 分析和相关测试验证，确认蓝牙驱动 RtkBtfilter.sys 引起蓝屏问题，删除 RtkBtfilter.sys 驱动可以正常启动设备。

问题分析：

当前 dump 显示蓝屏问题由蓝牙驱动 RtkBtfilter.sys 引起。相关分析情况如下:

dump 的 bugcheck code 为 7e，详细异常代码为 0xc0000005，这表示发生了内存访问冲突。

```
*******************************************************************************
*
*                        Bugcheck Analysis
*
*******************************************************************************

SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e)
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: ffffffffc0000005, The exception code that was not handled
Arg2: fffff8025dce1f22, The address that the exception occurred at
Arg3: fffff58934f8e5c8, Exception Record Address
Arg4: fffff58934f8de10, Context Record Address
```

```
BUGCHECK_CODE:  7e

BUGCHECK_P1: ffffffffc0000005

BUGCHECK_P2: fffff8025dce1f22

BUGCHECK_P3: fffff58934f8e5c8

BUGCHECK_P4: fffff58934f8de10

EXCEPTION_RECORD:  fffff58934f8e5c8 -- (.exr 0xfffff58934f8e5c8)
ExceptionAddress: fffff8025dce1f22 (Wdf01000!imp_WdfObjectGetTypedContextWorker+0x0000000000000042)
   ExceptionCode: c0000005 (Access violation)
  ExceptionFlags: 00000000
NumberParameters: 2
   Parameter[0]: 0000000000000000
   Parameter[1]: 0000000501000020
Attempt to read from address 0000000501000020
```

查看出问题的 call stack，在第 8 帧这里出现问题，抛出异常导致蓝屏。

```
1: kd> kn
 # Child-SP          RetAddr           Call Site
00 fffff589`34f8d5a8 fffff802`41fdf572 nt!KeBugCheckEx
01 fffff589`34f8d5b0 fffff802`41fa158f nt!PspSystemThreadStartup$filt$0+0x44
02 fffff589`34f8d5f0 fffff802`41fcfebf nt!_C_specific_handler+0x9f
03 fffff589`34f8d660 fffff802`41e2f390 nt!RtlpExecuteHandlerForException+0xf
04 fffff589`34f8d690 fffff802`41ed19c4 nt!RtlDispatchException+0x430
05 fffff589`34f8dde0 fffff802`41fd8cc2 nt!KiDispatchException+0x144
06 fffff589`34f8e490 fffff802`41fd4fae nt!KiExceptionDispatch+0xc2
07 fffff589`34f8e670 fffff802`5dce1f22 nt!KiPageFault+0x42e
08 fffff589`34f8e800 fffff802`64a634df Wdf01000!imp_WdfObjectGetTypedContextWorker+0x42
09 fffff589`34f8e850 fffff802`64a63b57 RtkBtfilter+0x634df
0a fffff589`34f8e8e0 fffff802`64a63305 RtkBtfilter+0x63b57
0b fffff589`34f8e970 fffff802`64ac10fb RtkBtfilter+0x63305
0c fffff589`34f8e9b0 fffff802`5dd37821 RtkBtfilter+0xc10fb
0d (Inline Function) --------`-------- Wdf01000!FxDriverDeviceAdd::Invoke+0x64 [minkerne
0e fffff589`34f8f1c0 fffff802`5dd3773c Wdf01000!FxDriver::AddDevice+0xd1 [minkernel\wdf\
0f fffff589`34f8f5e0 fffff802`41f79daf Wdf01000!FxDriver::AddDevice+0x2c [minkernel\wdf\
10 fffff589`34f8f610 fffff802`42508646 nt!PpvUtilCallAddDevice+0x3b
11 fffff589`34f8f650 fffff802`424ee2db nt!PnpCallAddDevice+0x56
12 fffff589`34f8f6e0 fffff802`424ed16b nt!PipCallDriverAddDevice+0xc2f
13 fffff589`34f8f8a0 fffff802`424fa7ea nt!PipProcessDevNodeTree+0x1af
14 fffff589`34f8f960 fffff802`41f6a08d nt!PiProcessReenumeration+0x82
15 fffff589`34f8f9b0 fffff802`41f1831a nt!PnpDeviceActionWorker+0x1dd
16 fffff589`34f8fa70 fffff802`41eeb645 nt!ExpWorkerThread+0x16a
17 fffff589`34f8fb10 fffff802`41fce82c nt!PspSystemThreadStartup+0x55
18 fffff589`34f8fb60 00000000`00000000 nt!KiStartSystemThread+0x1c
```

第 8 帧的 Wdf01000 是系统提供的为基于框架的驱动程序的运行库，查看当前是哪个驱动使用了 Wdf01000。查看第 8 帧的具体信息。

```
1: kd> .frame /r 08; !mex.x
08 fffff589`34f8e800 fffff802`64a634df Wdf01000!imp_WdfObjectGetTypedContextWorker+0x42 [minkernel\wdf\frame
rax=ffffa101868a3000 rbx=0000000000000000 rcx=0000000501000000
rdx=00005efe7975cff8 rsi=fffff58934f8ea18 rdi=ffffa1018c7020d8
rip=fffff8025dce1f22 rsp=fffff58934f8e800 rbp=fffff58934f8e8a0
 r8=fffff80264a84078  r9=0000000000000000 r10=ffffa10186886de0
r11=fffff58934f8e7f0 r12=fffff80264a7fc00 r13=fffff80264a7fc00
r14=0000000000004000 r15=fffff58934f8ea18
iopl=0         nv up ei ng nz na pe nc
cs=0010  ss=0018  ds=002b  es=002b  fs=0053  gs=002b             efl=00000282
Wdf01000!imp_WdfObjectGetTypedContextWorker+0x42:
fffff802`5dce1f22 4c394120        cmp     qword ptr [rcx+20h],r8 ds:002b:00000005`01000020=????????????????
<unavailable>     DriverGlobals = <value unavailable>
@rdx              Handle = 0x00005efe`7975cff8
@r8               TypeInfo = 0xfffff802`64a84078
@rax              pObject = 0xffffa101`868a3000
<unavailable>     pGivenName = <value unavailable>
@rcx              pHeader = 0x00000005`01000000
@r10              pFxDriverGlobals = 0xffffa101`86886de0
```

看到第 8 帧访问到了无效的内存，查看其 _FX_DRIVER_GLOBALS

```
1: kd> !mex.ddt -n pFxDriverGlobals

dt -n pFxDriverGlobals () Recursive: [ -r1 -r2 -r ] Verbose Normal dt
================================================================================
Local var @ r10 Type _FX_DRIVER_GLOBALS*
   +0x000 Linkage              : _LIST_ENTRY [ 0xffffa101`7eeeb050 - 0xffffa101`82c36dc0 ]
   +0x010 Refcnt               : 0n1
   +0x018 DestroyEvent         : MxEvent
   +0x038 WdfHandleMask        : 0xffffffff`fffffff8 (0n-8)
   +0x040 WdfVerifierAllocateFailCount : 0n-1
   +0x044 Tag                  : 0x426b7452 (0n1114338386) Tag: RtkB
   +0x048 Driver               : 0xffffa101`82eff1d0 FxDriver
   +0x050 DebugExtension       : (null)
   +0x058 LibraryGlobals       : 0xfffff802`5dd8bc20 FxLibraryGlobalsType
   +0x060 WdfLogHeader         : 0xffffa101`82fa9000 Void  PoolTag: FxLg
   +0x068 FxPoolFrameworks     : FX_POOL
   +0x108 FxPoolTrackingOn     : 0 ''
   +0x110 ThreadTableLock      : MxLock
   +0x120 ThreadTable          : (null)
   +0x128 WdfBindInfo          : 0xfffff802`64aac9e0 _WDF_BIND_INFO
   +0x130 ImageAddress         : 0xfffff802`64a00000 Void  [generic address]
   +0x138 ImageSize            : 0xcf000 (0n847872)
   +0x13c FxVerifierOn         : 0 ''
   +0x13d FxVerifyDownlevel    : 0 ''
   +0x13e FxVerifierDbgBreakOnError : 0 ''
   +0x13f FxVerifierDbgBreakOnDeviceStateError : 0 ''
   +0x140 FxVerifierHandle     : 0 ''
```

查找其对应的 FxDriver

```
1: kd> !mex.ddt 0xffffa101`82eff1d0 FxDriver

dt 0xffffa101`82eff1d0 FxDriver () Recursive: [ -r1 -r2 -r ] Verbose Normal dt
================================================================================
Wdf01000!FxDriver
   +0x000 __VFN_table          : 0xfffff802`5dd78d78
   +0x008 m_Type               : 0x1001 (0n4097)
   +0x00a m_ObjectSize         : 0x170 (0n368)
   +0x00c m_Refcnt             : 0n1
   +0x010 m_Globals            : 0xffffa101`86886de0 _FX_DRIVER_GLOBALS
   +0x018 m_ObjectFlags        : 0xc1b (0n3099)
   +0x018 m_ObjectFlagsByName  : FxObject::<unnamed-tag>::<unnamed-type-m_ObjectFlagsByName>
   +0x01a m_ObjectState        : 1
   +0x020 m_ChildListHead      : _LIST_ENTRY [ 0xffffa101`82f77408 - 0xffffa101`8680e068 ]
   +0x030 m_SpinLock           : MxLock
   +0x040 m_ParentObject       : (null)
   +0x048 m_ChildEntry         : _LIST_ENTRY [ 0xffffa101`82eff218 - 0xffffa101`82eff218 ] [EMPTY OR 1 ELEMENT]
   +0x058 m_DisposeSingleEntry : _SINGLE_LIST_ENTRY
   +0x060 m_DeviceBase         : (null)
   +0x060 m_Device             : (null)
   +0x068 m_NPLock             : MxLock
   +0x078 __VFN_table          : 0xfffff802`5dd78db8
   +0x080 m_DriverObject       : MxDriverObject
   +0x088 m_RegistryPath       : _UNICODE_STRING "\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\RtkBtFilter"
   +0x098 m_DebuggerConnected  : 0 ''
   +0x0a0 m_DriverDeviceAdd    : FxDriverDeviceAdd
   +0x0b0 m_ExecutionLevel     : 3 ( WdfExecutionLevelDispatch )
   +0x0b4 m_SynchronizationScope : 4 ( WdfSynchronizationScopeNone )
```

查看 RtkBtfilter 具体信息

```
1: kd> lmvm RtkBtFilter
Browse full module list
start             end                 module name
fffff802`64a00000 fffff802`64acf000   RtkBtfilter    (no symbols)
    Loaded symbol image file: RtkBtfilter.sys
    Image path: \SystemRoot\System32\drivers\RtkBtfilter.sys
    Image name: RtkBtfilter.sys
    Browse all global symbols  functions  data
    Timestamp:        Wed Nov 20 16:02:04 2019 (5DD4F2FC)
    CheckSum:         000C8BD1
    ImageSize:        000CF000
    Translations:     0000.04b0 0000.04e4 0409.04b0 0409.04e4
    Information from resource tables:
```

RtkBtfilter.sys 是 RealTek 的蓝牙驱动，这个驱动是 2019 年的版本。

处理建议：

通过日志分析和实际测试情况，判断新的 TMS 分组策略与三方驱动 RtkBtfilter.sys 兼容性问题导致蓝屏，有如下建议：

1) 禁用蓝牙设备，并删除蓝牙驱动 RtkBtfilter.sys，或者请硬件设备厂商提供新的蓝牙驱动 RtkBtfilter.sys 验证运行情况。
2) 请 TMS 厂商协助分析与蓝牙驱动 RtkBtfilter.sys 兼容性问题。

以上，如您后续有任何问题，可随时与我们联系，谢谢。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

发件人: Wei Liang
发送时间: 2021 年 12 月 7 日 16:12
收件人: '邓凯' <dengkai@yn.icbc.com.cn>; 'win10sup@sdc.icbc.com.cn' <win10sup@sdc.icbc.com.cn>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: 回复:【外来邮件，注意核实】回复: [案例号：CAS-05219-P5W5M3] % |P2|ICBC|分行安装补丁后调整 TMS 分组蓝屏协助分析 % 初次响应 CMIT:0001357

附件的日志收集工具，请查收。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

发件人: Wei Liang
发送时间: 2021 年 12 月 7 日 15:23
收件人: '邓凯' <dengkai@yn.icbc.com.cn>; win10sup@sdc.icbc.com.cn
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: 回复:【外来邮件，注意核实】回复: [案例号: CAS-05219-P5W5M3] % |P2|ICBC|分行安装补丁后调整 TMS 分组蓝屏协助分析 % 初次响应 CMIT:0001357

邓先生 & 吴先生 你们好:

感谢电话接听。

此次电话沟通情况总结如下:

1) 行内禁止使用电脑蓝牙设备，但是**未确认新的 TMS 分组具体安全策略管控信息。**
2) 查看了几台未出现蓝屏问题的计算机，其蓝牙设备厂家均是 Intel，蓝牙驱动显示为损坏状态。
3) 出现蓝屏的计算机，使用 PE 删除蓝牙驱动 RtkBtfilter.sys，可以正常运行，但域用户丢失，只剩 ICBC 用户。

通过日志分析和实际测试情况，判断新的 TMS 分组策略与三方驱动 RtkBtfilter.sys 兼容性问题导致蓝屏，有如下建议:

1) 禁用蓝牙设备，并删除蓝牙驱动 RtkBtfilter.sys。
2) 请 TMS 厂商协助分析与蓝牙驱动 RtkBtfilter.sys 兼容性问题。

您所说的删除蓝牙设备后，出现域用户丢失的问题，请您下载附件中的 CMGELogCollector.zip，解压后运行，勾选全部选项，点击“收集”，运行几分钟后会在桌面生成日志压缩包。

将上述操作收取的日志上传到 sftp 服务器，我们会尝试分析域用户丢失问题。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

发件人: 邓凯 <dengkai@yn.icbc.com.cn>
发送时间: 2021 年 12 月 7 日 11:21
收件人: Wei Liang <weiliang@cmgos.com>
抄送: win10 升级支持_系统一部_软件开发中心 <win10sup@sdc.icbc.com.cn>; ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复:【外来邮件，注意核实】回复: [案例号: CAS-05219-P5W5M3] % |P2|ICBC|分行安装补丁后调整 TMS 分组蓝屏协助分析 % 初次响应 CMIT:0001357

两个 dump 显示问题都是 RtkBtfilter.sys 引起。蓝屏问题在调整 TMS 分组后出现，请您确认 TMS 相关配置并进行一些测试：

1) 确认新的 TMS 分组对**蓝牙设备的安全策略管控**情况。

2) 其他未出现蓝屏问题的计算机是否有蓝牙设备？如果有蓝牙，**蓝牙设备的生产厂家**是什么，如 RealTek 还是 Intel，对应的**蓝牙驱动版本**是多少。

3) 已经出现蓝屏的一体机，请您使用 PE 进入操作系统分区**删除蓝牙驱动 RtkBtfilter.sys**，验证设备是否正常运行。（操作系统分区目录

1)需要咨询中心安全部门，分行不知晓策略详细内容。

2）找了几台设备，包括笔记本和老型号一体机，目前看来蓝牙均为 intel，蓝牙驱动显示为损坏状态。

3）使用 PE 删除驱动后设备可正常运行，但域用户丢失，只剩 ICBC 用户。

-----原始邮件-----

发件人: "Wei Liang" <weiliang@cmgos.com>
发送时间: 2021-12-02 15:52:12
收件人: "邓凯" <邓凯.云南分行金融科技部@工商银行.icbc>
抄送: "win10 升级支持_系统一部_软件开发中心" <win10sup@sdc.icbc.com.cn>,"ICBC_Notification" <icbc_notification@cmgos.com>
主题: 【外来邮件，注意核实】回复: [案例号: CAS-05219-P5W5M3] % |P2|ICBC|分行安装补丁后调整 TMS 分组蓝屏协助分析 % 初次响应 CMIT:0001357

邓先生 您好:

感谢您的电话接听。

当前 dump 显示蓝屏问题由蓝牙驱动 RtkBtfilter.sys 引起。相关分析情况如下:

dump 的 bugcheck code 为 7e，详细异常代码为 0xc0000005，这表示发生了内存访问冲突。

```
*******************************************************************************
*
*                        Bugcheck Analysis
*
*******************************************************************************

SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e)
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: ffffffffc0000005, The exception code that was not handled
Arg2: fffff8025dce1f22, The address that the exception occurred at
Arg3: fffff58934f8e5c8, Exception Record Address
Arg4: fffff58934f8de10, Context Record Address

BUGCHECK_CODE:  7e

BUGCHECK_P1: ffffffffc0000005

BUGCHECK_P2: fffff8025dce1f22

BUGCHECK_P3: fffff58934f8e5c8

BUGCHECK_P4: fffff58934f8de10

EXCEPTION_RECORD:  fffff58934f8e5c8 -- (.exr 0xfffff58934f8e5c8)
ExceptionAddress: fffff8025dce1f22 (Wdf01000!imp_WdfObjectGetTypedContextWorker+0x0000000000000042)
   ExceptionCode: c0000005 (Access violation)
  ExceptionFlags: 00000000
NumberParameters: 2
   Parameter[0]: 0000000000000000
   Parameter[1]: 0000000501000020
Attempt to read from address 0000000501000020
```

查看出问题的 call stack，在第 8 帧这里出现问题，抛出异常导致蓝屏。

```
1: kd> kn
 # Child-SP          RetAddr           Call Site
00 fffff589`34f8d5a8 fffff802`41fdf572 nt!KeBugCheckEx
01 fffff589`34f8d5b0 fffff802`41fa158f nt!PspSystemThreadStartup$filt$0+0x44
02 fffff589`34f8d5f0 fffff802`41fcfebf nt!_C_specific_handler+0x9f
03 fffff589`34f8d660 fffff802`41e2f390 nt!RtlpExecuteHandlerForException+0xf
04 fffff589`34f8d690 fffff802`41ed19c4 nt!RtlDispatchException+0x430
05 fffff589`34f8dde0 fffff802`41fd8cc2 nt!KiDispatchException+0x144
06 fffff589`34f8e490 fffff802`41fd4fae nt!KiExceptionDispatch+0xc2
07 fffff589`34f8e670 fffff802`5dce1f22 nt!KiPageFault+0x42e
08 fffff589`34f8e800 fffff802`64a634df Wdf01000!imp_WdfObjectGetTypedContextWorker+0x42
09 fffff589`34f8e850 fffff802`64a63b57 RtkBtfilter+0x634df
0a fffff589`34f8e8e0 fffff802`64a63305 RtkBtfilter+0x63b57
0b fffff589`34f8e970 fffff802`64ac10fb RtkBtfilter+0x63305
0c fffff589`34f8e9b0 fffff802`5dd37821 RtkBtfilter+0xc10fb
0d (Inline Function) --------`-------- Wdf01000!FxDriverDeviceAdd::Invoke+0x64 [minkerne
0e fffff589`34f8f1c0 fffff802`5dd3773c Wdf01000!FxDriver::AddDevice+0xd1 [minkernel\wdf\
0f fffff589`34f8f5e0 fffff802`41f79daf Wdf01000!FxDriver::AddDevice+0x2c [minkernel\wdf\
10 fffff589`34f8f610 fffff802`42508646 nt!PpvUtilCallAddDevice+0x3b
11 fffff589`34f8f650 fffff802`424ee2db nt!PnpCallAddDevice+0x56
12 fffff589`34f8f6e0 fffff802`424ed16b nt!PipCallDriverAddDevice+0xc2f
13 fffff589`34f8f8a0 fffff802`424fa7ea nt!PipProcessDevNodeTree+0x1af
14 fffff589`34f8f960 fffff802`41f6a08d nt!PiProcessReenumeration+0x82
15 fffff589`34f8f9b0 fffff802`41f1831a nt!PnpDeviceActionWorker+0x1dd
16 fffff589`34f8fa70 fffff802`41eeb645 nt!ExpWorkerThread+0x16a
17 fffff589`34f8fb10 fffff802`41fce82c nt!PspSystemThreadStartup+0x55
18 fffff589`34f8fb60 00000000`00000000 nt!KiStartSystemThread+0x1c
```

第 8 帧的 Wdf01000 是系统提供的为基于框架的驱动程序的运行库，查看当前是哪个驱动使用了 Wdf01000。查看第 8 帧的具体信息。

```
1: kd> .frame /r 08; !mex.x
08 fffff589`34f8e800 fffff802`64a634df Wdf01000!imp_WdfObjectGetTypedContextWorker+0x42 [minkernel\wdf\frame
rax=ffffa101868a3000 rbx=0000000000000000 rcx=0000000501000000
rdx=00005efe7975cff8 rsi=fffff58934f8ea18 rdi=ffffa1018c7020d8
rip=fffff8025dce1f22 rsp=fffff58934f8e800 rbp=fffff58934f8e8a0
 r8=fffff80264a84078  r9=0000000000000000 r10=ffffa10186886de0
r11=fffff58934f8e7f0 r12=fffff80264a7fc00 r13=fffff80264a7fc00
r14=0000000000004000 r15=fffff58934f8ea18
iopl=0         nv up ei ng nz na pe nc
cs=0010  ss=0018  ds=002b  es=002b  fs=0053  gs=002b             efl=00000282
Wdf01000!imp_WdfObjectGetTypedContextWorker+0x42:
fffff802`5dce1f22 4c394120        cmp     qword ptr [rcx+20h],r8 ds:002b:00000005`01000020=????????????????
<unavailable>     DriverGlobals = <value unavailable>
@rdx              Handle = 0x00005efe`7975cff8
@r8               TypeInfo = 0xfffff802`64a84078
@rax              pObject = 0xffffa101`868a3000
<unavailable>     pGivenName = <value unavailable>
@rcx              pHeader = 0x00000005`01000000
@r10              pFxDriverGlobals = 0xffffa101`86886de0
```

看到第 8 帧访问到了无效的内存，查看其 _FX_DRIVER_GLOBALS

```
1: kd> !mex.ddt -n pFxDriverGlobals

dt -n pFxDriverGlobals () Recursive: [ -r1 -r2 -r ] Verbose Normal dt
================================================================================
Local var @ r10 Type _FX_DRIVER_GLOBALS*
   +0x000 Linkage              : _LIST_ENTRY [ 0xffffa101`7eeeb050 - 0xffffa101`82c36dc0 ]
   +0x010 Refcnt               : 0n1
   +0x018 DestroyEvent         : MxEvent
   +0x038 WdfHandleMask        : 0xffffffff`fffffff8 (0n-8)
   +0x040 WdfVerifierAllocateFailCount : 0n-1
   +0x044 Tag                  : 0x426b7452 (0n1114338386) Tag: RtkB
   +0x048 Driver               : 0xffffa101`82eff1d0 FxDriver
   +0x050 DebugExtension       : (null)
   +0x058 LibraryGlobals       : 0xfffff802`5dd8bc20 FxLibraryGlobalsType
   +0x060 WdfLogHeader         : 0xffffa101`82fa9000 Void  PoolTag: FxLg
   +0x068 FxPoolFrameworks     : FX_POOL
   +0x108 FxPoolTrackingOn     : 0 ''
   +0x110 ThreadTableLock      : MxLock
   +0x120 ThreadTable          : (null)
   +0x128 WdfBindInfo          : 0xfffff802`64aac9e0 _WDF_BIND_INFO
   +0x130 ImageAddress         : 0xfffff802`64a00000 Void  [generic address]
   +0x138 ImageSize            : 0xcf000 (0n847872)
   +0x13c FxVerifierOn         : 0 ''
   +0x13d FxVerifyDownlevel    : 0 ''
   +0x13e FxVerifierDbgBreakOnError : 0 ''
   +0x13f FxVerifierDbgBreakOnDeviceStateError : 0 ''
   +0x140 FxVerifierHandle     : 0 ''
```

查找其对应的 FxDriver

```
1: kd> !mex.ddt 0xffffa101`82eff1d0 FxDriver

dt 0xffffa101`82eff1d0 FxDriver () Recursive: [ -r1 -r2 -r ] Verbose Normal dt
================================================================================
Wdf01000!FxDriver
   +0x000 __VFN_table          : 0xfffff802`5dd78d78
   +0x008 m_Type               : 0x1001 (0n4097)
   +0x00a m_ObjectSize         : 0x170 (0n368)
   +0x00c m_Refcnt             : 0n1
   +0x010 m_Globals            : 0xffffa101`86886de0 _FX_DRIVER_GLOBALS
   +0x018 m_ObjectFlags        : 0xc1b (0n3099)
   +0x018 m_ObjectFlagsByName  : FxObject::<unnamed-tag>::<unnamed-type-m_ObjectFlagsByName>
   +0x01a m_ObjectState        : 1
   +0x020 m_ChildListHead      : _LIST_ENTRY [ 0xffffa101`82f77408 - 0xffffa101`8680e068 ]
   +0x030 m_SpinLock           : MxLock
   +0x040 m_ParentObject       : (null)
   +0x048 m_ChildEntry         : _LIST_ENTRY [ 0xffffa101`82eff218 - 0xffffa101`82eff218 ] [EMPTY OR 1 ELEMENT]
   +0x058 m_DisposeSingleEntry : _SINGLE_LIST_ENTRY
   +0x060 m_DeviceBase         : (null)
   +0x060 m_Device             : (null)
   +0x068 m_NPLock             : MxLock
   +0x078 __VFN_table          : 0xfffff802`5dd78db8
   +0x080 m_DriverObject       : MxDriverObject
   +0x088 m_RegistryPath       : _UNICODE_STRING "\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\RtkBtFilter"
   +0x098 m_DebuggerConnected  : 0 ''
   +0x0a0 m_DriverDeviceAdd    : FxDriverDeviceAdd
   +0x0b0 m_ExecutionLevel     : 3 ( WdfExecutionLevelDispatch )
   +0x0b4 m_SynchronizationScope : 4 ( WdfSynchronizationScopeNone )
```

查看 RtkBtfilter 具体信息

```
1: kd> lmvm RtkBtFilter
Browse full module list
start             end                 module name
fffff802`64a00000 fffff802`64acf000   RtkBtfilter   (no symbols)
    Loaded symbol image file: RtkBtfilter.sys
    Image path: \SystemRoot\System32\drivers\RtkBtfilter.sys
    Image name: RtkBtfilter.sys
    Browse all global symbols  functions  data
    Timestamp:        Wed Nov 20 16:02:04 2019 (5DD4F2FC)
    CheckSum:         000C8BD1
    ImageSize:        000CF000
    Translations:     0000.04b0 0000.04e4 0409.04b0 0409.04e4
    Information from resource tables:
```

RtkBtfilter.sys 是 RealTek 的蓝牙驱动，这个驱动是 2019 年的版本。

两个 dump 显示问题都是 RtkBtfilter.sys 引起。蓝屏问题在调整 TMS 分组后出现，请您确认 TMS 相关配置并进行一些测试：

1) 确认新的 TMS 分组对**蓝牙设备的安全策略管控**情况。
2) 其他未出现蓝屏问题的计算机是否有蓝牙设备？如果有蓝牙，**蓝牙设备的生产厂家**是什么，如 RealTek 还是 Intel，对应的**蓝牙驱动版本**是多少。
3) 已经出现蓝屏的一体机，请您使用 PE 进入操作系统分区**删除蓝牙驱动 RtkBtfilter.sys**，验证设备是否正常运行。（操作系统分区目录 \windows\system32\drivers\RtkBtfilter.sys）。
4) 请您测试删除**蓝牙驱动 RtkBtfilter.sys** 后，再加入新的 TMS 分组是否出现蓝屏。（C:\windows\system32\drivers\RtkBtfilter.sys）。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

发件人: Wei Liang
发送时间: 2021 年 12 月 1 日 15:23
收件人: 'dengkai@yn.icbc.com.cn' <dengkai@yn.icbc.com.cn>
抄送: '吴毓杰' <win10sup@sdc.icbc.com.cn>; ICBC_Notification <ICBC_Notification@cmgos.com>

主题: 回复: [案例号: CAS-05219-P5W5M3] % |P2|ICBC|分行安装补丁后调整 TMS 分组蓝屏协助分析 % 初次响应 CMIT:0001357

邓先生 您好:

请您使用 Filezilla 软件，使用以下账户信息登入神州网信网站上传 dump 日志。

Filezilla client 端下载 URL：https://filezilla-project.org/download.php?type=client

登陆地址：sftp://ocean.cmgos.com

用户名为：ICBC（区分大小写）

密码：2qfs52ninbFB

端口：22222

登陆之后，**导航至/upload/**，新建一个新文件夹重命名为 **TMS 分组蓝屏**，再上传 dump 日志。

==========

在向 CMIT 提供日志和数据前，请阅读并接受邮件下方隐私声明。

隐私声明

为向您提供本产品的相关技术支持及相关服务，您需要在同意本声明的前提下向神州网信提供为解决系统故障必要的数据和信息，包括但不限于与您相关的个人数据和隐私信息。通常情况下，我们仅需要如下数据以使我们的服务能够更好地满足您的需求：内存转储文件、注册表信息、组策略信息、事件日志、安装应用列表、驱动信息、网络日志或系统补丁等。

神州网信承诺将采取商业上可行及必要措施保护用户提供给神州网信的数据和信息，且仅在解决问题过程中使用。

神州网信保证不对外公开或向第三方提供、公开或共享您提供的数据和信息。

在以下情况下，神州网信对您的数据和信息的披露将不视为违约，具体包括:

(1) 神州网信已获得您的明确授权;

(2) 根据适用法律的要求，神州网信负有披露义务的;

(3) 司法机关或行政机关基于法定程序要求神州网信提供的；

(4) 为维护社会公共利益及神州网信合法权益，在合理范围内进行披露的。

(5) 为了解决您的系统故障问题，神州网信可能会与神州网信的分包商披露您提供的数据和信息。在此情况下，第三方会承担与神州网信同等的隐私保护责任的，神州网信会在合理范围内对您的信息进行披露。

如果您欲提供的数据和信息中包含对您重要的保密信息以及商业秘密，在您向神州网信提供上述数据和信息前，务必对上述数据和信息进行脱敏处理，否则请不要提供该信息给神州网信。作为一家商业软件公司，神州网信在商业可行的前提下，已为用户的数据和信息保护做了极大的努力，但是仍然不能保证现有的安全技术措施使您的数据和信息等不受任何形式的损失。您对上述情况充分知情，且不会因此追究神州网信的法律责任。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

发件人: Wei Liang
发送时间: 2021 年 12 月 1 日 11:38
收件人: 'dengkai@yn.icbc.com.cn' <dengkai@yn.icbc.com.cn>
抄送: '吴毓杰' <win10sup@sdc.icbc.com.cn>; ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: [案例号：CAS-05219-P5W5M3] % |P2|ICBC|分行安装补丁后调整 TMS 分组蓝屏协助分析 % 初次响应 CMIT:0001357

邓先生 您好：

按照您提供的邮箱再发送一次，请您查收。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

发件人: Wei Liang
发送时间: 2021 年 12 月 1 日 11:23
收件人: '000887420@yn.icbc' <000887420@yn.icbc>
抄送: 吴毓杰 <win10sup@sdc.icbc.com.cn>; ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: [案例号: CAS-05219-P5W5M3] % |P2|ICBC|分行安装补丁后调整 TMS 分组蓝屏协助分析 % 初次响应 CMIT:0001357

邓先生 您好:

根据刚才的电话沟通，我谨在此阐述我们双方针对这个问题所涉及范围界定:

问题定义:

工行云南行一体机安装 11 月补丁，调整 TMS 分组后，出现蓝屏问题。

问题范围:

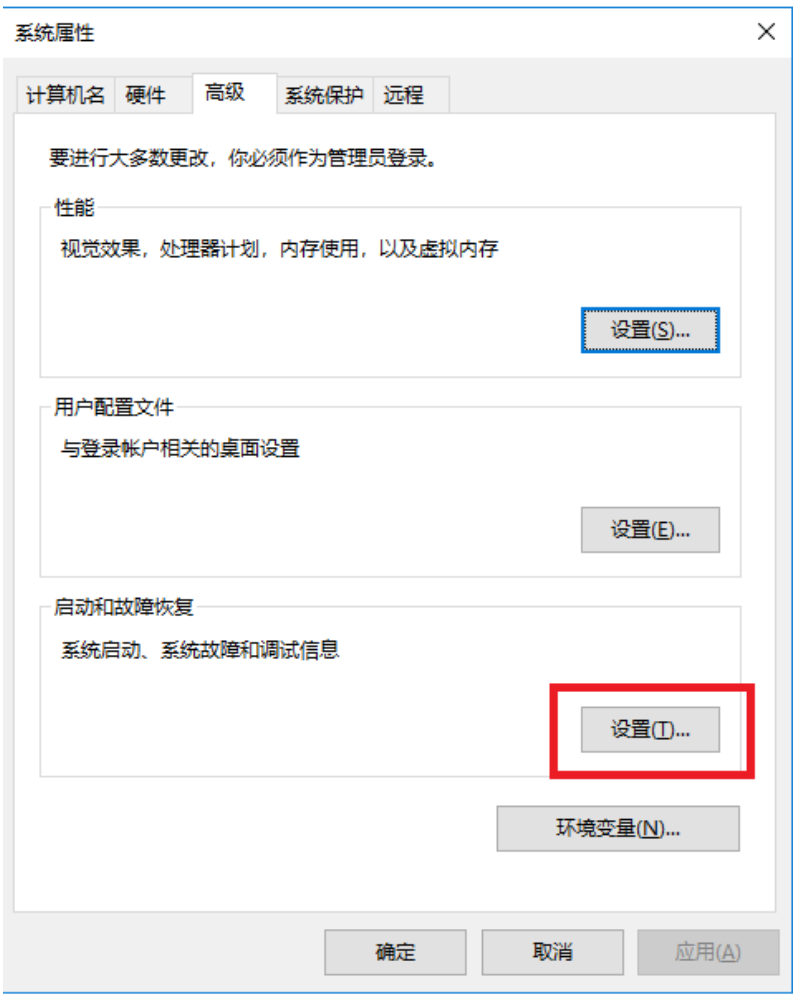
我们将协助您分析处理上述问题，并对定义的问题给予最大的技术支持。
如果能及时解决问题，或问题属于产品设计的行为，或问题涉及到三方，我们将考虑关闭案例。如果存在多个问题，则我们考虑拆分案例进行分析。

接下来，我们将开始合作解决这个问题。如果您对以上的问题范围界定有任何异议，请尽快告知。如果您有其他任何疑问。也欢迎随时与我联系。

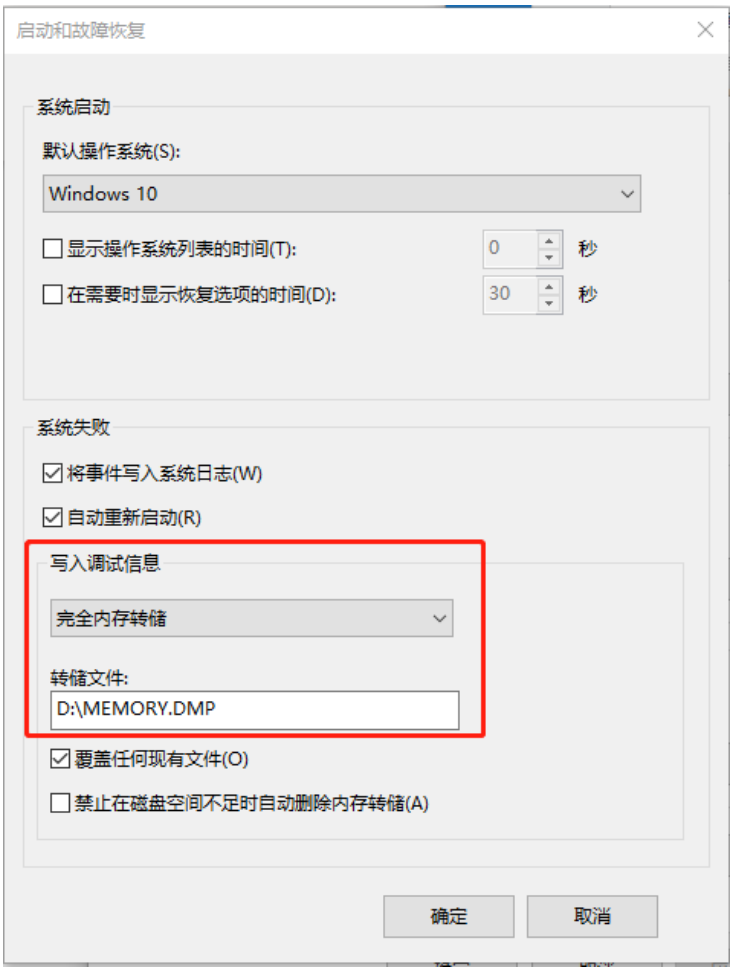
在出现蓝屏重启后，默认会在系统文件夹 Window 目录下生成 MEMORY.DMP 文件，如没有生成对应的 dmp 文件，请您在出现蓝屏前，按照以下方式配置蓝屏自动生成 dmp 文件。
1）右键点击此电脑，然后点击属性。

2）点击控制面板下面的高级系统设置。

3）在“系统属性“下面的”启动和故障恢复“里面，选择"设置“。



4)在“启动和故障恢复“界面内的”写入调试信息“部分，点击下拉菜单选择”**完全内存转储**“将转储文件改为其他本地磁盘，例如 D:\MEMORY.DMP，因为完全内存转储所需的空间较大，为当前计算机的内存大小。



当再次出现蓝屏的时候，等待**生成 dump** 文件。

基于您所说**出现蓝屏后，无法进入系统，只能通过 PE 复制文件，请您复制以下文件：**

通过 PE 进入系统后，访问操作系统分区，复制相关文件。

1）复制 Windows 目录下的 MEMORY.DMP 文件。

2）复制 Windows\System32\winevt\Logs 目录下的所有文件。

将对应的文件压缩，请麻烦 @吴毓杰 帮忙上传到 sftp 服务器。

==========

在向 CMIT 提供日志和数据前，请阅读并接受邮件下方隐私声明。

隐私声明

为向您提供本产品的相关技术支持及相关服务，您需要在同意本声明的前提下向神州网信提供为解决系统故障必要的数据和信息，包括但不限于与您相关的个人数据和隐私信息。通常情况下，我们仅需要如下数据以使我们的服务能够更好地满足您的需求：内存转储文件、注册表信息、组策略信息、事件日志、安装应用列表、驱动信息、网络日志或系统补丁等。

神州网信承诺将采取商业上可行及必要措施保护用户提供给神州网信的数据和信息，且仅在解决问题过程中使用。

神州网信保证不对外公开或向第三方提供、公开或共享您提供的数据和信息。

在以下情况下，神州网信对您的数据和信息的披露将不视为违约，具体包括:

(1) 神州网信已获得您的明确授权;

(2) 根据适用法律的要求，神州网信负有披露义务的;

(3) 司法机关或行政机关基于法定程序要求神州网信提供的;

(4) 为维护社会公共利益及神州网信合法权益，在合理范围内进行披露的。

(5) 为了解决您的系统故障问题，神州网信可能会与神州网信的分包商披露您提供的数据和信息。在此情况下，第三方会承担与神州网信同等的隐私保护责任的，神州网信会在合理范围内对您的信息进行披露。

如果您欲提供的数据和信息中包含对您重要的保密信息以及商业秘密，在您向神州网信提供上述数据和信息前，务必对上述数据和信息进行脱敏处理，否则请不要提供该信息给神州网信。作为一家商业软件公司，神州网信在商业可行的前提下，已为用户的数据和信息保护做了极大的努力，但是仍然不能保证现有的安全技术措施使您的数据和信息等不受任何形式的损失。您对上述情况充分知情，且不会因此追究神州网信的法律责任。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

神州网信
CMIT

发件人: Wei Liang <weiliang@cmgos.com>
发送时间: 2021 年 12 月 1 日 10:36

收件人: 吴毓杰 <win10sup@sdc.icbc.com.cn>
抄送: Wei Liang <weiliang@cmgos.com>
主题: [案例号: CAS-05219-P5W5M3] % |P2|ICBC|分行安装补丁后调整 TMS 分组蓝屏协助分析 % 初次响应 CMIT:0001357

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 危亮 。 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-05219-P5W5M3 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”。