Hi 李经理，李琦

感谢反馈，经过您的确认，接下来我将临时归档本案，如果后续您还有相关问题需要协助，欢迎再次电话或者邮件与我们沟通，我可以重启 case 来协助您跟踪问题。

华斌
Support Escalation Eng | Microsoft China Co Ltd | +86 (510) 66657739 | bihua@microsoft.com

---

From: Li Qi <liqi@cmgos.com>
Sent: Tuesday, September 15, 2020 3:48 PM
To: Bin Hua <bihua@microsoft.com>; Li Xin <lixin@cmgos.com>; Li Zhang <zhaling@microsoft.com>
Cc: Tony Ma (CSAM) <yima@microsoft.com>; support <support@mail.support.microsoft.com>; Wxepscov <Wxepscov@microsoft.com>; winnet <winprcnet@microsoft.com>; CRM Case Email <casemail@cmgos.com>; Wang Wenlei <wangwl@cmgos.com>; Bo Chen <Bo.Chen@microsoft.com>; Yucong Jiang <yucji@microsoft.com>
Subject: [外部] 回复: [REG:120081126000849] CAS-02698-C5V4N5 - 升级 1809 后从网盘拷文件蓝屏

Hi，华工:

这个 case 暂时不需要后续跟进，暂时可以关了。感谢支持。

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: Bin Hua <bihua@microsoft.com>
发送时间: 2020 年 8 月 28 日 20:53
收件人: Li Qi <liqi@cmgos.com>; Li Xin <lixin@cmgos.com>; Li Zhang <zhaling@microsoft.com>
抄送: Tony Ma (CSAM) <yima@microsoft.com>; support <support@mail.support.microsoft.com>; Wxepscov <Wxepscov@microsoft.com>; winnet <winprcnet@microsoft.com>; CRM Case Email <casemail@cmgos.com>; Wang Wenlei <wangwl@cmgos.com>; Bo Chen <Bo.Chen@microsoft.com>; Yucong Jiang

<yucji@microsoft.com>
主题: Re: [REG:120081126000849] CAS-02698-C5V4N5 - 升级 1809 后从网盘拷文件蓝屏

Hi 李经理，李琦

如电话沟通，您暂时没有进一步需要解释的问题了。我会把案件等级设置为 B，如需进一步协助，请与我联系。

BRs/Bin

From: Bin Hua
Sent: Friday, August 28, 2020 7:48:31 PM
To: 琦 李 <liqi@cmgos.com>; Li Xin <lixin@cmgos.com>; Li Zhang <zhaling@microsoft.com>
Cc: Tony Ma (CSAM) <yima@microsoft.com>; support <support@mail.support.microsoft.com>; Wxepscov <Wxepscov@microsoft.com>; winnet <winprcnet@microsoft.com>; CRM Case Email <casemail@cmgos.com>; Wang Wenlei <wangwl@cmgos.com>; Bo Chen <Bo.Chen@microsoft.com>; Yucong Jiang <yucji@microsoft.com>
Subject: RE: [REG:120081126000849] CAS-02698-C5V4N5 - 升级 1809 后从网盘拷文件蓝屏

Hi 李经理，

以下是基于 memory-copy.dmp 的详细分析，供两位参考。
其中的 dump 分析使用的均是原生命令，除了一个 mex.tag 用于根据 pool tag 找驱动名称。
如客户没有安装 mex，可以通过如下方法来找驱动名称: :
https://support.microsoft.com/en-sg/help/298102/how-to-find-pool-tags-that-are-used-by-third-party-drivers

Dump 分析:

- bugcheck 1e 是由于异常(exception)引起的蓝屏重启。触发异常的类型在 arg 1 0x80000003(STATUS_BREAKPOINT)

参考连接:
Analyze 命令： https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/using-the--analyze-extension
Bugcheck 1e: https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/bug-check-0x1e--kmode-exception-not-handled

```
2: kd> !analyze -v
*******************************************************************************
*
*
*
*                        Bugcheck
Analysis                                        *
```

```
*
*
*******************************************************************************
*

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
```

- 打出 call stack，在第 0x10 帧出现了地址 0x3200360035

参考连接：

k 命令：https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/k--kb--kc--kd--kp--kp--kv--display-stack-backtrace-

```
2: kd> k
 # Child-
SP          RetAddr               Call Site

00 ffff8401`32bdd808 fffff801`40745107     nt!KeBugCheckEx+0x0
01 ffff8401`32bdd810 fffff801`406841b6     nt!KiFatalFilter+0x1f
02 ffff8401`32bdd850 fffff801`4064554f     nt!KeExpandKernelStackAndCallou
tInternal$filt$0+0x16
03 ffff8401`32bdd890 fffff801`40673b5f     nt!__C_specific_handler+0x9f
04 ffff8401`32bdd900 fffff801`405cc450     nt!RtlpExecuteHandlerForExcepti
on+0xf
05 ffff8401`32bdd930 fffff801`404d9c24     nt!RtlDispatchException+0x430
06 ffff8401`32bde080 fffff801`4067c9c2     nt!KiDispatchException+0x144
07 ffff8401`32bde730 fffff801`40676681     nt!KiExceptionDispatch+0xc2
08 ffff8401`32bde910 fffff801`404e6236     nt!KiBreakpointTrap+0x301

09 ffff8401`32bdeaa0 fffff801`406454eb     nt!KeCheckStackAndTargetAddress
+0x46
0a ffff8401`32bdead0 fffff801`40673b5f     nt!__C_specific_handler+0x3b
0b ffff8401`32bdeb40 fffff801`405cc450     nt!RtlpExecuteHandlerForExcepti
on+0xf
0c ffff8401`32bdeb70 fffff801`404d9c24     nt!RtlDispatchException+0x430
0d ffff8401`32bdf2c0 fffff801`4067c9c2     nt!KiDispatchException+0x144
0e ffff8401`32bdf970 fffff801`40678cae     nt!KiExceptionDispatch+0xc2
0f ffff8401`32bdfb50 00000032`00360035     nt!KiPageFault+0x42e

10 ffff8401`32bdfce8 fffff801`3ed59513     0x3200360035
11 ffff8401`32bdfcf0 fffff801`3ed5d66d     nwifi!Dot11SendCompletion+0x4b
```

```
12 ffff8401`32bdfd30 fffff801`43b766a3     nwifi!Pt6SendComplete+0x1d
13 ffff8401`32bdfd60 fffff801`43b784ce     ndis!ndisCallSendCompleteHandle
r+0x33
14 ffff8401`32bdfda0 fffff801`40597a78     ndis!ndisDataPathExpandStackCal
lback+0x3e
15 ffff8401`32bdfdf0 fffff801`405979ed     nt!KeExpandKernelStackAndCallou
tInternal+0x78
16 ffff8401`32bdfe60 fffff801`43b9e104     nt!KeExpandKernelStackAndCallou
tEx+0x1d
17 (Inline Function) --------`--------     ndis!ndisExpandStack+0x65
18 (Inline Function) --------`-------
-     ndis!ndisExpandDataPathStack+0x65
19 (Inline Function) --------`-------
-     ndis!ndisInvokeNextSendCompleteHandler+0x28ba1
1a ffff8401`32bdfea0 fffff801`44641f92     ndis!NdisFSendNetBufferListsCom
plete+0x28dc4
1b ffff8401`32bdff90 fffff801`43b766a3     vwifimf+0x1f92
1c ffff8401`32bdffe0 fffff801`43b784ce     ndis!ndisCallSendCompleteHandle
r+0x33
1d ffff8401`32be0020 fffff801`40597a78     ndis!ndisDataPathExpandStackCal
lback+0x3e
1e ffff8401`32be0070 fffff801`405979ed     nt!KeExpandKernelStackAndCallou
tInternal+0x78
1f ffff8401`32be00e0 fffff801`43b9e104     nt!KeExpandKernelStackAndCallou
tEx+0x1d
20 (Inline Function) --------`--------     ndis!ndisExpandStack+0x65
```

- 进入到第 0x10 和 0x11 帧查看，发现 rax= 0000003200360035，rbx= ffffda8ad44db938

```
2: kd> .frame /r 0x10
10 ffff8401`32bdfce8 fffff801`3ed59513     0x00000032`00360035
rax=0000003200360035 rbx=ffffda8ad44db938 rcx=ffffda8acc2ec2c0
rdx=0000000000000000 rsi=ffffda8acc2ec2c0 rdi=ffffda8acdf28a30
rip=0000003200360035 rsp=ffff840132bdfce8 rbp=0000000000000000
r8=4c46444e02156700  r9=ec770c55eb0493df r10=ffffda8acc232320
r11=0000000000000001 r12=0000000000000000 r13=0000000000000004
r14=fffff80143b78490 r15=0000000000000000
iopl=0         nv up ei ng nz na pe nc
cs=0010  ss=0018  ds=002b  es=002b  fs=0053  gs=002b             efl=00000282
00000032`00360035 ??              ???
2: kd> .frame /r 0x11
11 ffff8401`32bdfcf0 fffff801`3ed5d66d     nwifi!Dot11SendCompletion+0x4b
rax=0000003200360035 rbx=ffffda8ad44db938 rcx=ffffda8acc2ec2c0
rdx=0000000000000000 rsi=ffffda8acc2ec2c0 rdi=ffffda8acdf28a30
rip=fffff8013ed59513 rsp=ffff840132bdfcf0 rbp=0000000000000000
r8=4c46444e02156700  r9=ec770c55eb0493df r10=ffffda8acc232320
r11=0000000000000001 r12=0000000000000000 r13=0000000000000004
r14=fffff80143b78490 r15=0000000000000000
iopl=0         nv up ei ng nz na pe nc
```

```
cs=0010  ss=0018  ds=002b  es=002b  fs=0053  gs=002b             efl=00000282
nwifi!Dot11SendCompletion+0x4b:
fffff801`3ed59513 4883eb18        sub     rbx,18h
```

- 查看第 0x11 帧的本地变量，其中 pTOS 的值存储在寄存器 rbx 中

dv 命令：https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/dv--display-local-variables-

```
2: kd> dv
    pNdisPacket = 0xffffda8a`cc2ec2c0
     ndisStatus = 0n0
           pBOS = 0xffffda8a`cdf28a30
           pTOS = 0xffffda8a`d44db938
```

- 通过 Windows 代码，我们知道 pTOS 的数据类型是 nwifi!DOT11_COMPLETION_STACK_ENTRY，打出 pTOS 的内部结构，pTOS 其中的一个字段 pRoutine 的地址是导致异常的 0x00000032`00360035，说明是 pTOS 的内容异常引起了蓝屏

dt 命令：https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/dt--display-type-

```
2: kd> dt ffffda8ad44db938 nwifi!DOT11_COMPLETION_STACK_ENTRY
   +0x000 pRoutine         : 0x00000032`00360035 Void
   +0x008 pCtxt            : 0x4c46444e`02156700 Void
   +0x010 pCtxt2           : 0xec770c55`eb0493df Void
```

- 通过 pool 和 tag 命令，找到了这个 NBL 包内存地址是由 vwifimf.sys 驱动申请和维护的。经客户确认，vwifimf.sys 是由三方软件 TMS 开发的驱动。

Pool 命令：https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/-pool

通过 pool tag 找三方驱动的方法：https://support.microsoft.com/en-sg/help/298102/how-to-find-pool-tags-that-are-used-by-third-party-drivers

```
2: kd> dt ffffda8acc2ec2c0 nwifi!_NET_BUFFER_LIST
   +0x000 Next             : (null)
   +0x008 FirstNetBuffer   : 0xffffda8a`cc2ec440 _NET_BUFFER
   +0x000 Link             : _SLIST_HEADER
   +0x000 NetBufferListHeader : _NET_BUFFER_LIST_HEADER
   +0x010 Context          : 0xffffda8a`cdf289f0 _NET_BUFFER_LIST_CONTEXT
   +0x018 ParentNetBufferList : (null)
   +0x020 NdisPoolHandle   : 0xffffda8a`c4ad8680 Void
   +0x030 NdisReserved     : [2] (null)
   +0x040 ProtocolReserved : [4] 0xffffda8a`d49982e0 Void
   +0x060 MiniportReserved : [2] (null)
   +0x070 Scratch          : (null)
   +0x078 SourceHandle     : 0xffffda8a`c4ad2660 Void
   +0x080 NblFlags         : 0
   +0x084 ChildRefCount    : 0n0
   +0x088 Flags            : 0x500
   +0x08c Status           : 0n0
   +0x08c NdisReserved2    : 0
   +0x090 NetBufferListInfo : [26] (null)

2: kd> !pool 0xffffda8ac4ad8680 2
Pool page ffffda8ac4ad8680 region is Nonpaged pool
```

```
*ffffda8ac4ad8650 size:  600 previous size:    0  (Allocated) *Filt
                Owning component : Unknown (update pooltag.txt)


2: kd> !mex.tag Filt
Name    Number of Hits Version Time Stamp          Location
======= ============== ======= ==================
=========================================
vwifimf              1 0.0.0.0 06/23/2020 03:10:42
\SystemRoot\system32\DRIVERS\vwifimf.sys

Hits
=============================================
fffff801`44641790  41 b8 46 69 6c 74 03 d1-0f b7 08 8d 94 0a 08
01  A.Filt.........
```

Best regards,
Bin Hua

From: Bin Hua <bihua@microsoft.com>
Sent: Monday, August 24, 2020 5:55 PM
To: 琦 李 <liqi@cmgos.com>; Li Xin <lixin@cmgos.com>; Li Zhang <zhaling@microsoft.com>
Cc: Tony Ma (CSAM) <yima@microsoft.com>; support <support@mail.support.microsoft.com>; Wxepscov <Wxepscov@microsoft.com>; winnet <winprcnet@microsoft.com>; CRM Case Email <casemail@cmgos.com>; Wang Wenlei <wangwl@cmgos.com>; Bo Chen <Bo.Chen@microsoft.com>; Yucong Jiang <yucji@microsoft.com>
Subject: RE: [REG:120081126000849] CAS-02698-C5V4N5 - 升级 1809 后从网盘拷文件蓝屏

Hi 李琦,

感谢确认，接下来我将暂时归档本案，如果后续您还有相关问题需要协助，欢迎再次电话或者邮件与我们沟通，我可以重启 case 来协助您跟踪问题。

华斌
Support Escalation Eng | Microsoft China Co Ltd | +86 (510) 66657739 | bihua@microsoft.com

---

From: Li Qi <liqi@cmgos.com>
Sent: Monday, August 24, 2020 10:29 AM
To: Bin Hua <bihua@microsoft.com>; Li Xin <lixin@cmgos.com>; Li Zhang <zhaling@microsoft.com>
Cc: Tony Ma (CSAM) <yima@microsoft.com>; support <support@mail.support.microsoft.com>; Wxepscov <Wxepscov@microsoft.com>; winnet <winprcnet@microsoft.com>; CRM Case Email <casemail@cmgos.com>;

Wang Wenlei <wangwl@cmgos.com>; Bo Chen <Bo.Chen@microsoft.com>; Yucong Jiang <yucji@microsoft.com>
Subject: [外部] 回复: [REG:120081126000849] CAS-02698-C5V4N5 - 升级 1809 后从网盘拷文件蓝屏

Hi, Hua Bin:

此 case 已与用户沟通，可以暂时归档，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: Bin Hua <bihua@microsoft.com>
发送时间: 2020 年 8 月 24 日 9:56
收件人: Li Qi <liqi@cmgos.com>; Li Xin <lixin@cmgos.com>; Li Zhang <zhaling@microsoft.com>
抄送: Tony Ma (CSAM) <yima@microsoft.com>; support <support@mail.support.microsoft.com>; Wxepscov <Wxepscov@microsoft.com>; winnet <winprcnet@microsoft.com>; CRM Case Email <casemail@cmgos.com>; Wang Wenlei <wangwl@cmgos.com>; Bo Chen <Bo.Chen@microsoft.com>; Yucong Jiang <yucji@microsoft.com>
主题: RE: [REG:120081126000849] CAS-02698-C5V4N5 - 升级 1809 后从网盘拷文件蓝屏

Hi 李琦,

循例跟进下本案，请问这个 case 贵方是否有什么进展？谢谢!

华斌
Support Escalation Eng | Microsoft China Co Ltd | +86 (510) 66657739 | bihua@microsoft.com

From: Bin Hua <bihua@microsoft.com>
Sent: Wednesday, August 19, 2020 4:52 PM
To: 琦 李 <liqi@cmgos.com>; 'Li Xin' <lixin@cmgos.com>; Li Zhang <zhaling@microsoft.com>
Cc: Tony Ma (CSAM) <yima@microsoft.com>; support <support@mail.support.microsoft.com>; Wxepscov <Wxepscov@microsoft.com>; winnet <winprcnet@microsoft.com>; 'CRM Case Email' <casemail@cmgos.com>; 'Wang Wenlei' <wangwl@cmgos.com>; Bo Chen <Bo.Chen@microsoft.com>; Yucong Jiang <yucji@microsoft.com>
Subject: RE: [REG:120081126000849] CAS-02698-C5V4N5 - 升级 1809 后从网盘拷文件蓝屏

Hi 李琦,

8 月 18 号的蓝屏 dump MEMORY-copy，问题原因和之前相同,都是 pTOS 数据异常引起的蓝屏重启。
了解到 vwifimf.sys 是 TMS 的无线组件，建议 TMS 厂商进一步排查。

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 C
ontextSwitches Wait Reason Time State
```

```
System (ffffda8ac4a63200) ffffda8ac6402080 4.d0            0s     8s.828
         59916 Executive     0s Running on CPU 2

 # Child-
SP         Return           Call Site                                 In
fo
 0 ffff840132bdd808 fffff80140745107 nt!KeBugCheckEx+0x0

 1 ffff840132bdd810 fffff801406841b6 nt!KiFatalFilter+0x1f

 2 ffff840132bdd850 fffff8014064554f nt!KeExpandKernelStackAndCalloutInter
nal$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 ? ]
```

华斌
Support Escalation Eng | Microsoft China Co Ltd | +86 (510) 66657739 | bihua@microsoft.com

---

From: Bin Hua
Sent: Wednesday, August 19, 2020 10:36 AM
To: 琦 李 <liqi@cmgos.com>; 'Li Xin' <lixin@cmgos.com>; Li Zhang <zhaling@microsoft.com>
Cc: Tony Ma (CSAM) <yima@microsoft.com>; support <support@mail.support.microsoft.com>; Wxepscov <Wxepscov@microsoft.com>; winnet <winprcnet@microsoft.com>; 'CRM Case Email' <casemail@cmgos.com>; 'Wang Wenlei' <wangwl@cmgos.com>; Bo Chen <Bo.Chen@microsoft.com>; Yucong Jiang <yucji@microsoft.com>
Subject: RE: [REG:120081126000849] CAS-02698-C5V4N5 - 升级 1809 后从网盘拷文件蓝屏

Hi 李琦,

8 月 11 号的 first-dump，问题原因经过代码工程师确认与 8 月 17 号收集的 1803 版本蓝屏原因相同，都是 pTOS 数据异常引起的蓝屏重启。

下一步建议:

卸载 vwifimf.sys 驱动，或引入 vwifimf.sys 的驱动厂商进一步排查 NBL 的 pTOS 参数设置。

Dump 分析:
Bugcheck 0xfc，在不可执行的内存空间 fffff8032addb290 执行命令，导致了蓝屏。

```
ATTEMPTED_EXECUTE_OF_NOEXECUTE_MEMORY (fc)
An attempt was made to execute non-executable memory.  The guilty driver
is on the stack trace (and is typically the current instruction pointer).
When possible, the guilty driver's name (Unicode string) is printed on
the bugcheck screen and saved in KiBugCheckDriver.
Arguments:
Arg1: fffff8032addb290, Virtual address for the attempted execute.
Arg2: 89000002284fe863, PTE contents.
Arg3: fffff08f489f4b50, (reserved)
Arg4: 0000000000000002, (reserved)
```

Callstack

```
1: kd> kc
# Call Site
00 nt!KeBugCheckEx
01 nt!MiCheckSystemNxFault
02 nt!MiSystemFault
03 nt!MmAccessFault
04 nt!KiPageFault
05 tcpip!Ipv4Global
06 nwifi!Dot11SendCompletion
07 nwifi!Pt6SendComplete
08 ndis!ndisCallSendCompleteHandler
09 ndis!ndisDataPathExpandStackCallback
0a nt!KeExpandKernelStackAndCalloutInternal
0b nt!KeExpandKernelStackAndCalloutEx
```

- 内存空间 fffff8032addb290 存放的是数据体 **pTOS 的参数 pRoutine**, 通过查看 pTOS 所在内存地址 0xffff8102`1744d1b0 是由三方迷你网卡过滤驱动（mini-port filter driver）vwifimf.sys 维护的。

```
1: kd> .frame /r 0x5; !mex.x
05 fffff08f`489f4ce8 fffff803`2f869513     tcpip!Ipv4Global
rax=fffff8032addb290 rbx=fffff08f489eb3b0 rcx=ffff810210913d90
rdx=0000000000000000 rsi=ffff810210913d90 rdi=ffff81021744d1e0
rip=fffff8032addb290 rsp=fffff08f489f4ce8 rbp=0000000000000000
r8=ffffb08061b864f0  r9=0000000000000001 r10=ffff81020f092880
r11=0000000000000001 r12=0000000000000000 r13=000000000000002c
r14=fffff8032a9a8490 r15=0000000000000000
iopl=0         nv up ei pl zr na po nc
```

```
cs=0010  ss=0018  ds=002b  es=002b  fs=0053  gs=002b
efl=00000246
tcpip!Ipv4Global:
fffff803`2addb290 0100            add     dword ptr [rax],eax
ds:002b:fffff803`2addb290=00000001

1: kd> .frame 0n6; !mex.x
06 fffff08f`489f4cf0
fffff803`2f86d66d     nwifi!Dot11SendCompletion+0x4b
@rsi              pNdisPacket = 0xffff8102`10913d90
@ebp              ndisStatus = 0n0
@rdi              pBOS = 0xffff8102`1744d1e0
@rbx              pTOS = 0xfffff08f`489eb3b0

1: 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                 : 0xfffff803`2addb290 Void
   +0x008 pCtxt                    : 0xffffb080`61b864f0 Void
   +0x010 pCtxt2                   : 0x00000000`00000001 Void

1: kd> dt 0xffff8102`10913d90 DOT11_PACKET
nwifi!DOT11_PACKET
   +0x000 Next             : (null)
   +0x008 FirstNetBuffer   : 0xffff8102`10913f10 _NET_BUFFER
   +0x000 Link             : _SLIST_HEADER
   +0x000 NetBufferListHeader : _NET_BUFFER_LIST_HEADER
   +0x010 Context          : 0xffff8102`1744d1a0
_NET_BUFFER_LIST_CONTEXT
   +0x018 ParentNetBufferList : (null)
   +0x020 NdisPoolHandle   : 0xffff8102`0f50f040 Void
   +0x030 NdisReserved     : [2] (null)
   +0x040 ProtocolReserved : [4] 0xffff8102`10181030 Void
   +0x060 MiniportReserved : [2] (null)
   +0x070 Scratch          : (null)
   +0x078 SourceHandle     : 0xffff8102`075046a0 Void
   +0x080 NblFlags         : 0
   +0x084 ChildRefCount    : 0n0
   +0x088 Flags            : 0x500
   +0x08c Status           : 0n0
   +0x08c NdisReserved2    : 0
   +0x090 NetBufferListInfo : [26] (null)
```

```
1: kd> !pool 0xffff8102`1744d1b0
Pool page ffff81021744d1b0 region is Nonpaged pool
ffff81021744d010 size:   30 previous
size:    0  (Allocated)  DSnd
ffff81021744d040 size:   30 previous
size:    0  (Allocated)  DSnd
ffff81021744d070 size:   30 previous
size:    0  (Allocated)  DSnd
ffff81021744d0a0 size:   30 previous size:    0  (Allocated)  Io
 ffff81021744d0d0 size:   30 previous
size:    0  (Allocated)  FSfc
ffff81021744d100 size:   30 previous
size:    0  (Allocated)  DSnd
ffff81021744d130 size:   30 previous
size:    0  (Free)       VWFF
ffff81021744d160 size:   30 previous
size:    0  (Free)       IoUs
*ffff81021744d190 size:   30 previous size:    0  (Allocated)
*Filt


1: kd> !tag Filt
Name    Number of Hits Version Time Stamp          Location
======= ============== ======= ==================
========================================
vwifimf              1 0.0.0.0 06/23/2020 03:10:42
\SystemRoot\system32\DRIVERS\vwifimf.sys

Hits
============================================
fffff803`2bb61790  41 b8 46 69 6c 74 03 d1-0f b7 08 8d 94 0a 08
01  A.Filt.........
```

华斌
Support Escalation Eng | Microsoft China Co Ltd | +86 (510) 66657739 | bihua@microsoft.com

---

From: Bin Hua <bihua@microsoft.com>
Sent: Monday, August 17, 2020 2:53 PM
To: 琦 李 <liqi@cmgos.com>; 'Li Xin' <lixin@cmgos.com>; Li Zhang <zhaling@microsoft.com>
Cc: Tony Ma (CSAM) <yima@microsoft.com>; support <support@mail.support.microsoft.com>; Wxepscov <Wxepscov@microsoft.com>;

winnet <winprcnet@microsoft.com>; 'CRM Case Email' <casemail@cmgos.com>; 'Wang Wenlei' <wangwl@cmgos.com>; Bo Chen <Bo.Chen@microsoft.com>; Yucong Jiang <yucji@microsoft.com>
Subject: RE: [REG:120081126000849] CAS-02698-C5V4N5 - 升级 1809 后从网盘拷文件蓝屏

Hi 李琦,

今天上午收集的 Windows 10 1803 版本的蓝屏已分析完毕，发现如下:

根据 call stack，在进行无线网络发送网络包时，发现网络包数据异常（内部数据 pTOS 为空）引起的蓝屏重启。
通过查看该网络包的内部结构，该内存地址 ffffe08f`6fa3fb20 是由三方迷你网卡过滤驱动（mini-port filter driver）vwifimf.sys 维护的。

下一步建议:
卸载 vwifimf.sys 驱动，或引入 vwifimf.sys 的驱动厂商进一步排查为何把 NBL 的 pTOS 参数设置为空。

Dump 分析:
Call Stack:

```
0: kd> kc
# Call Site
00 nt!KeBugCheckEx
01 nt!KiBugCheckDispatch
02 nt!KiPageFault
03 nwifi!Dot11SendCompletion
04 nwifi!Pt6SendComplete
05 ndis!ndisCallSendCompleteHandler
06 ndis!ndisIterativeDPInvokeHandlerOnTracker
07 ndis!ndisInvokeNextSendCompleteHandler
08 ndis!ndisMSendNetBufferListsCompleteInternal
09 ndis!NdisMSendNetBufferListsComplete
0a wdiwifi!CPort::SendCompleteNetBufferLists
0b wdiwifi!CAdapter::SendCompleteNbl
0c wdiwifi!CTxMgr::CompleteNdisNbl
0d wdiwifi!CTxMgr::CompleteNBLs
0e wdiwifi!CTxMgr::TxTransferCompleteInd
0f wdiwifi!AdapterTxTransferCompleteInd
10 Netwtw08
11 Netwtw08
12 Netwtw08
13 Netwtw08
14 Netwtw08
15 Netwtw08
16 Netwtw08
17 Netwtw08
```

```
0: kd> dt ffffe08f`6fa3fb20 DOT11_PACKET_CONTEXT
nwifi!DOT11_PACKET_CONTEXT
   +0x000 pVElan           : 0xffffe08f`70f738b0 _VELAN
   +0x008 pMacStateEntry   : 0x00000000`00001002 DOT11_MAC_STATE_ENTRY
   +0x010 uPriority        : 0x2080003
   +0x014 QoSInfo          : _DOT11_QOS_SEND_INFO
   +0x018 pvEthernetMediaSpecificInfo : 0xffff8a00`003b55c8 Void
   +0x020 bExcludeWEP      : 0n0
   +0x024 bDefaultKeyAllowed : 0n112
   +0x028 pTOS             : 0xffffe08f`6fa3fb50 DOT11_COMPLETION_STACK_ENTRY  //this
was Null when enter function nwifi!Dot11SendCompletion
   +0x030 CmplArray        : [16] DOT11_COMPLETION_STACK_ENTRY
   +0x1b0 SendExt          : _DOT11_SEND_CONTEXT
   +0x1b0 ExtSTASendExt    : DOT11_EXTSTA_SEND_CONTEXT
   +0x200 ExtV2            : _DOT11_SEND_EXTENSION_INFO_V2
   +0x206 ucExtRates       : [247]  ""
   +0x1b0 RecvExt          : _DOT11_RECV_CONTEXT
   +0x1b0 ExtSTARecvExt    : DOT11_EXTSTA_RECV_CONTEXT



Running: !mex.tag Filt
Name    Number of Hits Version Time Stamp          Location
======= ============== ======= ==================
=======================================
vwifimf              1 0.0.0.0 06/23/2020 03:10:42
\SystemRoot\system32\DRIVERS\vwifimf.sys
Hits
===========================================
fffff802`b97b1790  41 b8 46 69 6c 74 03 d1-0f b7 08 8d 94 0a 08 01  A.Filt..........
Search complete

kd> lmvm vwifimf
Browse full module list
start             end                 module name
fffff802`b97b0000 fffff802`b97ba000   vwifimf    (no symbols)
    Loaded symbol image file: vwifimf.sys
    Image path: \SystemRoot\system32\DRIVERS\vwifimf.sys
    Image name: vwifimf.sys
    Browse all global symbols  functions  data
    Timestamp:        Tue Jun 23 11:10:42 2020 (5EF172B2)
    CheckSum:         0000EDC3
    ImageSize:        0000A000
    Translations:     0000.04b0 0000.04e4 0409.04b0 0409.04e4
    Information from resource tables:


        (RASPPPOE)        ffffe08f7073dc10    Declined with NDIS_STATUS_FAILURE
      Filter list        Driver              Module              Context
        WFP 802.3 MAC Layer LightWeight Filter-0000
                          ffffe08f6a29bd60    ffffe08f6e7a9c60    ffffe08f6e7aa010
        QoS Packet Scheduler-0000
                          ffffe08f6a662a20    ffffe08f6e7bd010    ffffe08f6e7aa650
        Phenix NDIS LightWeight Filter-0000
                          ffffe08f6a7b27c0    ffffe08f6e796390    ffffe08f6e7b27d0
```

```
Native WiFi Filter Driver-0000
                    ffffe08f6e77ad70    ffffe08f6e798010    ffffe08f6e77b810
NDIS Sample LightWeight Filter 1-0000
                    ffffe08f6a61d7b0    ffffe08f6e793c60    ffffe08f6e793640
Virtual WiFi Filter Driver-0000
                    ffffe08f6a6327c0    ffffe08f6e78fc60    ffffe08f6e792010
WFP Native MAC Layer LightWeight Filter-0000
                    ffffe08f6a29bab0    ffffe08f6e773450    ffffe08f6e7f6940
```

华斌
Support Escalation Eng | Microsoft China Co Ltd | +86 (510) 66657739 | bihua@microsoft.com

---

From: Bin Hua
Sent: Thursday, August 13, 2020 5:56 PM
To: Li Qi <liqi@cmgos.com>; Bo Chen <Bo.Chen@microsoft.com>
Cc: Tony Ma (CSAM) <yima@microsoft.com>; support <support@mail.support.microsoft.com>; Wxepscov <Wxepscov@microsoft.com>; winnet <winprcnet@microsoft.com>; CRM Case Email <casemail@cmgos.com>; Yucong Jiang <yucji@microsoft.com>; Li Xin <lixin@cmgos.com>; Wang Wenlei <wangwl@cmgos.com>
Subject: RE: [REG:120081126000849] CAS-02698-C5V4N5 - 升级 1809 后从网盘拷文件蓝屏

Hi 李琦,

如电话所谈，第四次 dump bugcheck 与第三次不同，但两次 dump 出现 Error 0x80070057 表示 invalid parameter,说明 dump 中的部分信息损坏，无法解码出 call stack，与系统更新没有直接关系。
根据以往案例的最佳实践，建议客户有条件的情况下，升级 Windows 补丁到最新 KB 4559003（当前补丁状态是 2019 年 9 月）。

了解到第四次 dump 生成前客户尚未开启 special pool，建议客户开启后复现问题，再提供 dump 以便分析。

华斌
Support Escalation Eng | Microsoft China Co Ltd | +86 (510) 66657739 | bihua@microsoft.com

From: Li Qi <liqi@cmgos.com>
Sent: Wednesday, August 12, 2020 4:06 PM
To: Bin Hua <bihua@microsoft.com>; Bo Chen <Bo.Chen@microsoft.com>
Cc: Tony Ma (CSAM) <yima@microsoft.com>; support <support@mail.support.microsoft.com>; Wxepscov <Wxepscov@microsoft.com>; winnet <winprcnet@microsoft.com>; CRM Case Email <casemail@cmgos.com>; Yucong Jiang <yucji@microsoft.com>; Li Xin <lixin@cmgos.com>; Wang Wenlei <wangwl@cmgos.com>
Subject: [外部] 回复: [REG:120081126000849] CAS-02698-C5V4N5 - 升级 1809 后从网盘拷文件蓝屏

Hi, Hua Bin:

第四次的 dump 文件与系统日志已上传，和第三次的 dump 为同一台问题电脑，并且已经建议用户在这台电脑上开启 special pool，请知悉。
另外据了解，用户应该尚未更新补丁至最新，请从现有两个 dump 中帮忙分析是否与未更新完成有关，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: Bin Hua <bihua@microsoft.com>
发送时间: 2020 年 8 月 12 日 15:50
收件人: Li Qi <liqi@cmgos.com>; Bo Chen <Bo.Chen@microsoft.com>
抄送: Tony Ma (CSAM) <yima@microsoft.com>; support <support@mail.support.microsoft.com>; Wxepscov <Wxepscov@microsoft.com>; winnet <winprcnet@microsoft.com>; Yucong Jiang <yucji@microsoft.com>; Li Xin <lixin@cmgos.com>
主题: RE: [REG:120081126000849] CAS-02698-C5V4N5 - 升级 1809 后从网盘拷文件蓝屏

Hi 李琦,

感谢分析，确实 netwtw08.sys 驱动已经比较新了（2020 年 2 月），但也不能排除网卡驱动方面的原因，bugcheck D1 的蓝屏需要开启 special pool 后的 dump 来找到根本原因的。

工作空间地址如下:
====工作空间====
File Transfer - Case 120081126000849

华斌
Support Escalation Eng | Microsoft China Co Ltd | +86 (510) 66657739 | bihua@microsoft.com

---

From: Li Qi <liqi@cmgos.com>
Sent: Wednesday, August 12, 2020 3:40 PM
To: Bin Hua <bihua@microsoft.com>; Bo Chen <Bo.Chen@microsoft.com>
Cc: Tony Ma (CSAM) <yima@microsoft.com>; support <support@mail.support.microsoft.com>; Wxepscov <Wxepscov@microsoft.com>; winnet <winprcnet@microsoft.com>; Yucong Jiang <yucji@microsoft.com>; Li Xin <lixin@cmgos.com>
Subject: [外部] 回复: [REG:120081126000849] CAS-02698-C5V4N5 - 升级 1809 后从网盘拷文件蓝屏

Hi, Hua Bin:

感谢您的分析。
就您提到的第二次 dump 是因为访问了不可用的内存地址，是否有更多的 dump 信息可以分享。主要基于两点:

1. 该用户在之前与我们接触的 case 中，有过很多类似的蓝屏情况，但查看 bugcheck 这点来看，还未出现过 0XD1 的情况。
2. 我已经建议用户进行了网卡驱动的更新并保持最新。但目前用户还是出现了此次蓝屏情况。我不太清楚如果问题真的指向 Netwtw08.sys，还能做什么

另外有关于第二次 dump 的机器已经重装系统，并未再发生蓝屏现象，所以也没有办法再抓取 special pool

就您提到的第三次 dump 文件，我的分析是：bugcheck 为 0x50，在进行内存读操作时，也是访问了不可用的地址空间，导致蓝屏。查看 dx kibugcheckdriver 发现 80070057 error，所以我怀疑与系统更新有关。是否有这个可能原因?
这个我会建议用户开启 special pool 抓取。
另外第三次的机器现在又发生了蓝屏，稍后我也可以将新收集的 dump 日志发送给您，您方便的时候可以提供一个上传地址给我，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: Bin Hua <bihua@microsoft.com>
发送时间: 2020 年 8 月 12 日 14:54
收件人: Bo Chen <Bo.Chen@microsoft.com>; Li Qi <liqi@cmgos.com>
抄送: Tony Ma (CSAM) <yima@microsoft.com>; support <support@mail.support.microsoft.com>; Wxepscov <Wxepscov@microsoft.com>; winnet <winprcnet@microsoft.com>; Yucong Jiang <yucji@microsoft.com>
主题: RE: [REG:120081126000849] CAS-02698-C5V4N5 - 升级 1809 后从网盘拷文件蓝屏

Hi 李琦,

感谢日志收集，三个 dump 已下载并初步看了 call stack，第一个 dump 的具体的蓝屏原因还在分析中。
更新下当前最新的初步分析:

- 第二次 bugcheck 为 0XD1 的蓝屏，原因是某一个内存 pool 已经在蓝屏发生之前被破坏了，因此无线网络 nwifi 组件去访问的时候发生了错误。因为这是在访问之前发生的，不能确定是不是 nwifi 的问题。我们建议使用 driver verifier 去跟踪查看是哪个驱动破坏了这块内存。
  另外，根据 callstack，发送无线网络包的过程中涉及了三方网卡驱动 Netwtw08.sys，很有可能访问的内存地址之前是无线网卡申请的内存空间。

- 第三次是无线环境下拷贝数据的蓝屏，系统蓝屏 bugcheck 50（page fault）的原因是 page fault 内存错误引用。建议使用 driver verifier 去跟踪查看是哪个驱动最先破坏了这块内存。

基于以上的初步分析，三个 dump 的 call stack 都不同，触发蓝屏引起的原因也可能不同，建议根据不同症状新开两个案件单独追踪。

针对第二和第三个蓝屏 dump，下一步的日志收集方案：建议在问题机器上打开 special pool，并复现蓝屏收集新的 dump 日志

==========

1. 使用 driver verifier 启用 special pool，来分析那个进程损坏了内存 pool

special pool 启用步骤:

-. 运行命令 verifier，打开 Driver Verifier Manager

-. 选择 Create Standard Settings

-. 选择 Select driver names from a list

-. 选中 wdiwifi.sys,nwifi.sys, ndis.sys, tcpip.sys 以及第三方驱动（比如网卡 Netwtw08，杀毒软件等的驱动）

-. 点击 finish

-. 重启机器生效

三个 dump 的 bugcheck

```
ATTEMPTED_EXECUTE_OF_NOEXECUTE_MEMORY (fc)
An attempt was made to execute non-executable memory.  The guilty driver
is on the stack trace (and is typically the current instruction pointer).
When possible, the guilty driver's name (Unicode string) is printed on
the bugcheck screen and saved in KiBugCheckDriver.
Arguments:
Arg1: fffff8032addb290, Virtual address for the attempted execute.
Arg2: 89000002284fe863, PTE contents.
Arg3: fffff08f489f4b50, (reserved)
Arg4: 0000000000000002, (reserved)
```

```
DRIVER_IRQL_NOT_LESS_OR_EQUAL (d1)
An attempt was made to access a pageable (or completely invalid) address at an
interrupt request level (IRQL) that is too high.  This is usually
caused by drivers using improper addresses.
If kernel debugger is available get stack backtrace.
Arguments:
Arg1: ffffffffffffffe8, memory referenced
Arg2: 0000000000000002, IRQL
Arg3: 0000000000000000, value 0 = read operation, 1 = write operation
Arg4: fffff8012f6d94fd, address which referenced memory
```

```
PAGE_FAULT_IN_NONPAGED_AREA (50)
Invalid system memory was referenced.  This cannot be protected by try-except.
Typically the address is just plain bad or it is pointing at freed memory.
Arguments:
Arg1: ffffffffffffffe8, memory referenced.
Arg2: 0000000000000000, value 0 = read operation, 1 = write operation.
Arg3: fffff8057b5694fd, If non-zero, the instruction address which referenced
the bad memory
         address.
Arg4: 0000000000000002, (reserved)
```

华斌

Support Escalation Eng | Microsoft China Co Ltd | +86 (510) 66657739 | bihua@microsoft.com

---

From: Bo Chen <Bo.Chen@microsoft.com>
Sent: Wednesday, August 12, 2020 1:20 PM
To: 琦 李 <liqi@cmgos.com>; Bin Hua <bihua@microsoft.com>
Cc: Tony Ma (CSAM) <yima@microsoft.com>; support <support@mail.support.microsoft.com>; Wxepscov <Wxepscov@microsoft.com>
Subject: RE: [REG:120081126000849] CAS-02698-C5V4N5 - 升级 1809 后从网盘拷文件蓝屏

Hi 李琦,

Loop Network engineer @Bin Hua in this case thread, thanks!

此致,
敬礼!

Bo Chen
Tel: +86 510 6665 7857
My working hour *is (GMT+8:00) 9:00am~6:00pm, Monday to Friday. Thanks!*

From: Li Qi <liqi@cmgos.com>
Sent: 2020 年 8 月 11 日 15:46
To: Bo Chen <Bo.Chen@microsoft.com>
Cc: Tony Ma (CSAM) <yima@microsoft.com>; support <support@mail.support.microsoft.com>; Daniel Zhang <danzhan@microsoft.com>; Wxepscov <Wxepscov@microsoft.com>
Subject: [外部] 回复: [REG:120081126000849] CAS-02698-C5V4N5 - 升级 1809 后从网盘拷文件蓝屏

Hi,

Dump 已经上传，第一次怀疑为 DSP 版本问题造成的蓝屏，第二次为 bugcheck 为 0XD1 的蓝屏，第三次是无线环境下拷贝数据的蓝屏，请查收，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: Bo Chen <Bo.Chen@microsoft.com>
发送时间: 2020 年 8 月 11 日 13:08
收件人: Li Qi <liqi@cmgos.com>
抄送: Tony Ma (CSAM) <yima@microsoft.com>; support <support@mail.support.microsoft.com>; Daniel Zhang <danzhan@microsoft.com>; Wxepscov <Wxepscov@microsoft.com>
主题: [REG:120081126000849] CAS-02698-C5V4N5 - 升级 1809 后从网盘拷文件蓝屏

LiQi，您好!

感谢您致电微软全球技术中心。我是微软的技术支持工程师 Bo Chen，很高兴能有机会协助您解决该问题。您可随时通过以下联系方式以及该问题事件号码 120081126000849 与我联系。

刚刚有尝试拨打您的电话，未能成功接听。
从问题描述来看，目前为系统蓝屏 ，烦请参考如下建议收集日志，上传至空间，我会稍后再与您电话沟通，谢谢!

====下一步措施====
1．压缩上传 dump 文件
2．右击 cmd， 选择以管理员身份运行，运行以下命令行收集日志
msinfo32 /nfo C:\SYSSUM.NFO /categories +systemsummary
wevtutil epl System C:\system.evtx
wevtutil epl Application C:\app.evtx
wmic qfe list brief /format:htable > C:\hotfix.html
上传 C:\SYSSUM.NFO，C:\system.evtx，C:\app.evtx，C:\hotfix.html

====工作空间====

File Transfer - Case 120081126000849

liqi@cmgos.com
lixin@cmgos.com
casemail@cmgos.com

此致,
敬礼!

Bo Chen
Tel: +86 510 6665 7857
My working hour *is (GMT+8:00) 9:00am~6:00pm, Monday to Friday. Thanks!*