许先生 您好:

感谢您与 TAM 确认这个案例可以关闭，我将归档此案例。

工单的归档并不会影响我们为您提供技术支持服务，如有其他问题，您可以随时联系我们。

案例总结：

问题定义：

用户反馈林总的设备在公网环境下连接 vpn 出现异常蓝屏问题，需要协助分析。

问题总结：

通过分析提供的蓝屏 dump，显示 netmgr.sys 驱动触发了系统蓝屏，netmgr.sys 是 TMS 的组件，需要**三方应用厂商排查、处理其驱动问题**。

还有一次蓝屏显示是音频总线驱动 IntcDAud.sys 触发的蓝屏，此驱动程序是 2018 年的版本，建议通过硬件设备厂商官网下载**更新最新的音频总线驱动程序**。

此设备在以前处理蓝屏问题时，开启了 special pool 功能，**开启 special pool 容易暴露不太好的驱动的 bug。**可以通过以下操作**关闭 special pool 配置**。

以管理员权限打开 cmd 命令行，运行 **verifier.exe**，暂时关闭驱动程序验证工具，减少触发驱动的潜在问题的可能。

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: 2023 年 10 月 9 日 14:12
收件人: 'Soul power ギ' <303642690@qq.com>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: 回复： 回复: [案例号: CAS-09903-Z2V6L2] % |P2|ICBC|win10 异常蓝屏需要分析 % 初次响应 CMIT:0001387

许先生 您好:

刚刚给您的电话没有接通。

来信是想了解近期林总设备是否再次出现蓝屏问题，关于此案例是否仍有疑问?

如果有任何进展或疑问可以回复此邮件。

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: 2023 年 9 月 28 日 16:18
收件人: 'Soul power ギ' <303642690@qq.com>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: 回复: 回复: [案例号: CAS-09903-Z2V6L2] % |P2|ICBC|win10 异常蓝屏需要分析 % 初次响应 CMIT:0001387

许先生 您好:

分析您提供的最新的 dump 文件，它错误代码为 0x7e，指系统线程生成了错误处理程序未捕获的异常。

具体分析如下:

报错代码为 0x7e，第一个错误参数为 c000005，它表示 STATUS_ACCESS_VIOLATION，发生了内存访问冲突。

```
4: kd> !analyze -v
*******************************************************************************
*                                                                             *
*                        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: fffff80052e4a5be, The address that the exception occurred at
Arg3: ffffaf0da5589a98, Exception Record Address
Arg4: ffffaf0da5589ce0, Context Record Address

Debugging Details:
------------------
```

发生错误检查的原因是，系统线程中抛出异常，任何给定的异常处理程序都无法处理该异常。

检查 call stack，可以看到操作系统正在初始化一个系统线程。

```
4: kd> knL
 # Child-SP          RetAddr           Call Site
00 ffffaf0d`a5588a78 fffff803`459e81a4 nt!KeBugCheckEx
01 ffffaf0d`a5588a80 fffff803`459a9b0f nt!PspSystemThreadStartup$filt$0+0x44
02 ffffaf0d`a5588ac0 fffff803`459d891f nt!_C_specific_handler+0x9f
03 ffffaf0d`a5588b30 fffff803`4587a010 nt!RtlpExecuteHandlerForException+0xf
04 ffffaf0d`a5588b60 fffff803`4591d4d4 nt!RtlDispatchException+0x430
05 ffffaf0d`a55892b0 fffff803`459e16c2 nt!KiDispatchException+0x144
06 ffffaf0d`a5589960 fffff803`459dd9ae nt!KiExceptionDispatch+0xc2
07 ffffaf0d`a5589b40 fffff800`52e4a5be nt!KiPageFault+0x42e
08 ffffaf0d`a5589cd0 fffff800`52e6d6ab IntcDAud+0x3a5be
09 ffffaf0d`a5589d00 fffff800`52e6dba8 IntcDAud+0x5d6ab
0a ffffaf0d`a5589d90 fffff800`52e5a1a7 IntcDAud+0x5dba8
0b ffffaf0d`a5589de0 fffff800`52e7a9cb IntcDAud+0x4a1a7
0c ffffaf0d`a5589e40 fffff800`52e78dcf IntcDAud+0x6a9cb
0d ffffaf0d`a5589e90 fffff800`52e78d0a IntcDAud+0x68dcf
0e ffffaf0d`a5589ec0 fffff800`52e78598 IntcDAud+0x68d0a
0f ffffaf0d`a5589f60 fffff800`52e88cf4 IntcDAud+0x68598
10 ffffaf0d`a5589fc0 fffff800`525895ba IntcDAud+0x78cf4
11 ffffaf0d`a558a020 fffff800`525890ec portcls!iPowerChangeState+0x76
12 ffffaf0d`a558a060 fffff803`4589ab3d portcls!PowerIrpCompletionRoutine+0x39c
13 ffffaf0d`a558a0f0 fffff803`4589a957 nt!IopfCompleteRequest+0x1cd
14 ffffaf0d`a558a200 fffff800`4bc883e0 nt!IofCompleteRequest+0x17
15 (Inline Function) --------`-------- Wdf01000!FxIrp::CompleteRequest+0xc
16 (Inline Function) --------`-------- Wdf01000!FxPkgPnp::CompletePowerRequest+0x1f
17 ffffaf0d`a558a230 fffff800`4bc8075b Wdf01000!FxPkgPdo::PowerReleasePendingDeviceIrp+0x40
18 ffffaf0d`a558a260 fffff800`4bc818a7 Wdf01000!FxPkgPnp::PowerStartSelfManagedIo+0x2cb
19 (Inline Function) --------`-------- Wdf01000!FxPkgPnp::PowerEnterNewState+0x101
1a ffffaf0d`a558a2e0 fffff800`4bc80c6c Wdf01000!FxPkgPnp::PowerProcessEventInner+0x1f7
```

```
19 (Inline Function) --------`-------- Wdf01000!FxPkgPnp::PowerEnterNewState+0x101
1a ffffaf0d`a558a2e0 fffff800`4bc80c6c Wdf01000!FxPkgPnp::PowerProcessEventInner+0x1f7
1b ffffaf0d`a558a450 fffff800`4bc7fb23 Wdf01000!FxPkgPnp::PowerProcessEvent+0x15c
1c ffffaf0d`a558a4f0 fffff800`4bc7faa4 Wdf01000!FxPkgPdo::DispatchDeviceSetPower+0x77
1d ffffaf0d`a558a540 fffff800`4bc72ef4 Wdf01000!FxPkgPdo::_DispatchSetPower+0x24
1e ffffaf0d`a558a570 fffff800`4bc71b73 Wdf01000!FxPkgPnp::Dispatch+0xb4
1f (Inline Function) --------`-------- Wdf01000!DispatchWorker+0x9e
20 (Inline Function) --------`-------- Wdf01000!FxDevice::Dispatch+0xbc
21 ffffaf0d`a558a5e0 fffff803`459880e2 Wdf01000!FxDevice::DispatchWithLock+0x113
22 ffffaf0d`a558a640 fffff803`45892d90 nt!IopPoHandleIrp+0x36
23 ffffaf0d`a558a670 fffff803`4598c879 nt!IofCallDriver+0x70
24 ffffaf0d`a558a6b0 fffff800`4d347d12 nt!IoCallDriver+0x9
25 ffffaf0d`a558a6e0 fffff803`459880e2 devmgr+0x17d12
26 ffffaf0d`a558a730 fffff803`45892d90 nt!IopPoHandleIrp+0x36
27 ffffaf0d`a558a760 fffff803`4598c879 nt!IofCallDriver+0x70
28 ffffaf0d`a558a7a0 fffff800`525bfa24 nt!IoCallDriver+0x9
29 ffffaf0d`a558a7d0 fffff800`525b8de5 portcls!DispatchPower+0x484
2a ffffaf0d`a558a860 fffff800`52e1a320 portcls!PcDispatchIrp+0x3db5
2b ffffaf0d`a558a8d0 fffff803`459880e2 IntcDAud+0xa320
2c ffffaf0d`a558a930 fffff803`45892d90 nt!IopPoHandleIrp+0x36
2d ffffaf0d`a558a960 fffff803`4598c879 nt!IofCallDriver+0x70
2e ffffaf0d`a558a9a0 fffff800`52e016c8 nt!IoCallDriver+0x9
2f ffffaf0d`a558a9d0 fffff800`52e01023 ksthunk!CKernelFilterDevice::DispatchIrp+0x244
30 ffffaf0d`a558aa30 fffff803`45987ec6 ksthunk!CKernelFilterDevice::DispatchIrpBridge+0x13
31 ffffaf0d`a558aa60 fffff803`459363a5 nt!PopIrpWorker+0x226
32 ffffaf0d`a558ab10 fffff803`459d728c nt!PspSystemThreadStartup+0x55
33 ffffaf0d`a558ab60 00000000`00000000 nt!KiStartSystemThread+0x1c
```

从 call stack 中可以看到是 IntcDAud 触发了系统蓝屏。

```
4: kd> knL
 # Child-SP          RetAddr           Call Site
00 ffffaf0d`a5588a78 fffff803`459e81a4 nt!KeBugCheckEx
01 ffffaf0d`a5588a80 fffff803`459a9b0f nt!PspSystemThreadStartup$filt$0+0x44
02 ffffaf0d`a5588ac0 fffff803`459d891f nt!_C_specific_handler+0x9f
03 ffffaf0d`a5588b30 fffff803`4587a010 nt!RtlpExecuteHandlerForException+0xf
04 ffffaf0d`a5588b60 fffff803`4591d4d4 nt!RtlDispatchException+0x430
05 ffffaf0d`a55892b0 fffff803`459e16c2 nt!KiDispatchException+0x144
06 ffffaf0d`a5589960 fffff803`459dd9ae nt!KiExceptionDispatch+0xc2
07 ffffaf0d`a5589b40 fffff800`52e4a5be nt!KiPageFault+0x42e
08 ffffaf0d`a5589cd0 fffff800`52e6d6ab IntcDAud+0x3a5be
09 ffffaf0d`a5589d00 fffff800`52e6dba8 IntcDAud+0x5d6ab
0a ffffaf0d`a5589d90 fffff800`52e5a1a7 IntcDAud+0x5dba8
0b ffffaf0d`a5589de0 fffff800`52e7a9cb IntcDAud+0x4a1a7
0c ffffaf0d`a5589e40 fffff800`52e78dcf IntcDAud+0x6a9cb
```

再查看报错的几个参数，可以看到似乎异常是由驱动程序尝试使用完全无效的内存地址执行调用指令引起的。

```
4: kd> .cxr 0xffffaf0da55892e0
rax=ffffaf0da5589cf8 rbx=00000000c000023a rcx=fffff80052e27240
rdx=0000000000000003 rsi=0000000000000000 rdi=0000000000000000
rip=fffff80052e4a5be rsp=ffffaf0da5589cd0 rbp=ffffaf0da5589d50
 r8=ffffc701f8d59180  r9=0000000000000004 r10=ffffc701f8791180
r11=0000000000400000 r12=fffff80052e2700f r13=fffff80052e27048
r14=fffff80052e27048 r15=ffff9e8ebcf1c6a4
iopl=0         nv up ei pl zr na po nc
cs=0010  ss=0018  ds=002b  es=002b  fs=0053  gs=002b             efl=00010246
IntcDAud+0x3a5be:
fffff800`52e4a5be 40387e18        cmp     byte ptr [rsi+18h],dil ds:002b:00000000`00000018=??
```

使用 .exr 命令和错误检查的第三个参数的值转储该错误。

```
4: kd> .exr 0xffffaf0da5589a98
ExceptionAddress: fffff80052e4a5be (IntcDAud+0x000000000003a5be)
   ExceptionCode: c0000005 (Access violation)
  ExceptionFlags: 00000000
NumberParameters: 2
   Parameter[0]: 0000000000000000
   Parameter[1]: 0000000000000018
Attempt to read from address 0000000000000018
```

异常记录直接对应于在 call stack 中找到的内容。驱动程序 IntcDAud.sys 引用了前面显示的相同无效内存地址，这导致引发访问冲突错误。

IntcDAud.sys 是系统的音频驱动程序，其是 2018 年的驱动，建议升级音频驱动程序。

```
4: kd> lmvm IntcDAud
Browse full module list
start             end                 module name
fffff800`52e10000 fffff800`52eaa000   IntcDAud   (no symbols)
    Loaded symbol image file: IntcDAud.sys
    Image path: \SystemRoot\system32\DRIVERS\IntcDAud.sys
    Image name: IntcDAud.sys
    Browse all global symbols  functions  data
    Timestamp:        Wed Mar  7 21:43:09 2018 (5A9FEC6D)
    CheckSum:         000A3EC6
    ImageSize:        0009A000
    Translations:     0000.04b0 0000.04e4 0409.04b0 0409.04e4
    Information from resource tables:
```

下一步建议：

dump 日志显示是音频驱动程序导致的蓝屏，建议在设备厂商官网**更新最新的音频驱动**后，观察是否再次出现蓝屏问题。

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: Wei Liang
发送时间: 2023 年 9 月 28 日 15:39
收件人: 'Soul power ギ' <303642690@qq.com>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: 回复： 回复: [案例号: CAS-09903-Z2V6L2] % |P2|ICBC|win10 异常蓝屏需要分析 % 初次响应 CMIT:0001387

许先生 您好:

感谢您的电话接听。

分析您提供的最新 dump 文件，显示由于 bugcheck 代码为 **0xa**（IRQL_NOT_LESS_OR_EQUAL），这个错误检查是由使用不适当地址的内核模式设备驱动程序引起的。这个错误检查表明，在提高中断请求级别（IRQL）时，有人试图访问一个无效的地址。

发生了 0xa 的蓝屏，是由于读取了 IRQL 比较高的地址触发的。

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

IRQL_NOT_LESS_OR_EQUAL (a)
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 a kernel debugger is available get the stack backtrace.
Arguments:
Arg1: ffffe78a15047000, memory referenced
Arg2: 0000000000000002, IRQL
Arg3: 0000000000000000, bitfield :
      bit 0 : value 0 = read operation, 1 = write operation
      bit 3 : value 0 = not an execute operation, 1 = execute operation (only on chips which support this level of status)
Arg4: fffff8002044093b, address which referenced memory
```

查看出故障时的指令指针以及 irql 情况。

```
1: kd> ln fffff8002044093b
Browse module
Set bu breakpoint

(fffff800`204408f0)   nt!strstr+0x4b   |  (fffff800`20440950)   nt!atoi64
1: kd> !irql
Debugger saved IRQL for processor 0x1 -- 2 (DISPATCH_LEVEL)
```

查看 trap frame 情况，显示访问了无效的内存地址。

```
1: kd> .trap 0xfffff888f89ed8c0
NOTE: The trap frame does not contain all registers.
Some register values may be zeroed or incorrect.
rax=0000000000000048 rbx=0000000000000000 rcx=0000000000000075
rdx=fffff806000a1ab0 rsi=0000000000000000 rdi=0000000000000000
rip=fffff8002044093b rsp=fffff888f89eda58 rbp=00000000000007ec
 r8=ffffe78a15047000  r9=ffffef8414fa5550 r10=fffff806000a1ab0
r11=0000000000000000 r12=0000000000000000 r13=0000000000000000
r14=0000000000000000 r15=0000000000000000
iopl=0         nv up ei ng nz ac po nc
nt!strstr+0x4b:
fffff800`2044093b 418a00          mov     al,byte ptr [r8] ds:ffffe78a`15047000=??
```

查看出问题时的 call stack 情况，显示 netmgr.sys 驱动触发了 strstr 操作。

```
1: kd> knL
 # Child-SP          RetAddr           Call Site
00 fffff888`f89ed778 fffff800`204775e9 nt!KeBugCheckEx
01 fffff888`f89ed780 fffff800`204739d4 nt!KiBugCheckDispatch+0x69
02 fffff888`f89ed8c0 fffff800`2044093b nt!KiPageFault+0x454
03 fffff888`f89eda58 fffff806`0009cf15 nt!strstr+0x4b
04 fffff888`f89eda60 fffff806`0009dafc netmgr+0x1cf15
05 fffff888`f89edac0 fffff806`0009dc55 netmgr+0x1dafc
06 fffff888`f89edb00 fffff805`ffc09f57 netmgr+0x1dc55
07 fffff888`f89edb70 fffff805`ffc0c0d9 NETIO!ProcessCallout+0x907
08 fffff888`f89edd00 fffff805`ffc08971 NETIO!ArbitrateAndEnforce+0xba9
09 fffff888`f89edea0 fffff805`ffd953a8 NETIO!KfdClassify+0x561
0a fffff888`f89ee2b0 fffff805`ffd33250 tcpip!WfpTlShimInspectSendTcpDatagram+0x408
0b fffff888`f89ee470 fffff805`ffd324f5 tcpip!IppInspectLocalDatagramsOut+0x600
0c fffff888`f89ee760 fffff805`ffd31845 tcpip!IppSendDatagramsCommon+0x385
0d fffff888`f89ee8f0 fffff805`ffd0b221 tcpip!IpNlpFastSendDatagram+0x5c5
0e fffff888`f89ee9b0 fffff805`ffd09f2d tcpip!TcpTcbSend+0x12b1
0f fffff888`f89eed40 fffff805`ffd093f4 tcpip!TcpEnqueueTcbSend+0xb1d
10 fffff888`f89eee70 fffff800`202e0238 tcpip!TcpTlConnectionSendCalloutRoutine+0x24
11 fffff888`f89eeea0 fffff800`202e01ad nt!KeExpandKernelStackAndCalloutInternal+0x78
12 fffff888`f89eef10 fffff805`ffd5e017 nt!KeExpandKernelStackAndCalloutEx+0x1d
13 fffff888`f89eef50 fffff806`00b63b7f tcpip!TcpTlConnectionSend+0x77
```

netmgr 试图在一个 http 的网络连接地址的 string 里面查找 http/1.1 的 string。

```
1: kd> .frame /r 3
03 fffff888`f89eda58 fffff806`0009cf15 nt!strstr+0x4b
rax=0000000000000048 rbx=0000000000000000 rcx=0000000000000075
rdx=fffff806000a1ab0 rsi=0000000000000000 rdi=ffffe78a15046814
rip=fffff8002044093b rsp=fffff888f89eda58 rbp=00000000000007ec
 r8=ffffe78a15047000  r9=ffffef8414fa5550 r10=fffff806000a1ab0
r11=0000000000000000 r12=0000000000000001 r13=0000000000000000
r14=ffffe78a15046814 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
nt!strstr+0x4b:
fffff800`2044093b 418a00          mov     al,byte ptr [r8] ds:002b:ffffe78a`15047000=??
1: kd> .frame /r 4
04 fffff888`f89eda60 fffff806`0009dafc netmgr+0x1cf15
rax=0000000000000048 rbx=0000000000000000 rcx=0000000000000075
rdx=fffff806000a1ab0 rsi=0000000000000000 rdi=ffffe78a15046814
rip=fffff8060009cf15 rsp=fffff888f89eda60 rbp=00000000000007ec
 r8=ffffe78a15047000  r9=ffffef8414fa5550 r10=fffff806000a1ab0
r11=0000000000000000 r12=0000000000000001 r13=0000000000000000
r14=ffffe78a15046814 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
netmgr+0x1cf15:
fffff806`0009cf15 4c8bd8          mov     r11,rax
```

```
r14=ffffe78a15046814 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
netmgr+0x1cf15:
fffff806`0009cf15 4c8bd8          mov     r11,rax
1: kd> ub
netmgr+0x1cef2:
fffff806`0009cef2 488d150b860000  lea     rdx,[netmgr+0x25504 (fffff806`000a5504)]
fffff806`0009cef9 e86c300000      call    netmgr+0x1ff6a (fffff806`0009ff6a)
fffff806`0009cefe 85c0            test    eax,eax
fffff806`0009cf00 756c            jne     netmgr+0x1cf6e (fffff806`0009cf6e)
fffff806`0009cf02 488d15a74b0000  lea     rdx,[netmgr+0x21ab0 (fffff806`000a1ab0)]
fffff806`0009cf09 498bce          mov     rcx,r14
fffff806`0009cf0c 448d6601        lea     r12d,[rsi+1]
fffff806`0009cf10 e867300000      call    netmgr+0x1ff7c (fffff806`0009ff7c)
1: kd> dc fffff806`000a1ab0
fffff806`000a1ab0  50545448 312e312f 00000a0d 00000000  HTTP/1.1.......
fffff806`000a1ac0  20544547 70747468 002f2f3a 00000000  GET http://.....
fffff806`000a1ad0  4e4e4f43 20544345 00000000 00000000  CONNECT ........
fffff806`000a1ae0  6d74656e 23237267 6f745320 74784570  netmgr## StopExt
fffff806`000a1af0  616e7265 6e6f436c 7463656e 206e6f69  ernalConnection
fffff806`000a1b00  436c7452 61706d6f 654d6572 79726f6d  RtlCompareMemory
fffff806`000a1b10  69466220 3d20646e 55525420 00000a45   bFind = TRUE...
fffff806`000a1b20  6d74656e 23237267 6f745320 74784570  netmgr## StopExt
1: kd> dc ffffe78a15046814
ffffe78a`15046814  20544547 7665642f 6c6c6f63 2f746365  GET /devcollect/
ffffe78a`15046824  2f337066 666f7270 2e656c69 6e6f736a  fp3/profile.json
ffffe78a`15046834  7261703f 72656e74 6263693d 70612663  ?partner=icbc&ap
ffffe78a`15046844  616e5f70 463d656d 4d41412d 6b6f7426  p_name=F-AAM&tok
ffffe78a`15046854  695f6e65 63693d64 312d6362 38353936  en_id=icbc-16958
ffffe78a`15046864  35333436 31333937 3862372d 63363334  64357931-7b8436c
ffffe78a`15046874  33633965 61263834 4f71703d 4146376c  e9c348&a=pqOl7FA
ffffe78a`15046884  6b373975 38524a4e 67645036 344a4758  u97kNJR86PdgXGJ4
```

这个网络连接的 string 所在的地址有 special pool 的保护，系统捕捉到这个异常触发蓝屏。

```
1: kd> dc
ffffe78a`15046f94  39695758 48336d4c 6876386c 63383861  XWi9Lm3Hl8vha88c
ffffe78a`15046fa4  62785433 336d3677 68373443 61423225  3Txbw6m3C47h%2Ba
ffffe78a`15046fb4  68623165 46322535 53476559 6a594744  e1bh5%2FYeGSDGYj
ffffe78a`15046fc4  79654454 4e387450 37524444 48423225  TDeyPt8NDDR7%2BH
ffffe78a`15046fd4  46322543 496d3477 56775a58 7a786c78  C%2Fw4mIXZwVxlxz
ffffe78a`15046fe4  7271704b 6a585273 6c444a38 6d593150  KpqrsRXj8JDlP1Ym
ffffe78a`15046ff4  5a687667 724f6b6a 754d4d45 ????????  gvhZjkOrEMMu????
ffffe78a`15047004  ???????? ???????? ???????? ????????  ????????????????
```

```
1: kd> !pool ffffe78a15047000
Pool page ffffe78a15047000 region is Special pool
ffffe78a15047000: Unable to get contents of special pool block
```

注：所谓 special pool 的工作原理，可以通俗理解为，在相关组件的内存块上下增加了用户监控的 nonpaged pool 内存，如果有人触及这段内存，就会直接触发蓝屏，得到问题发生现场的 dump。special pool 容易暴露不太好的驱动的 bug。

林总这台设备在以前处理蓝屏问题时开启过 special pool，针对 ndis.sys、netmgr.sys、vwifimf.sys 和 nwifi.sys 驱动开启了驱动程序验证。

```
1: kd> !verifier

Verify Flags Level 0x00100001

  STANDARD FLAGS:
    [X] (0x00000000) Automatic Checks
    [X] (0x00000001) Special pool
    [ ] (0x00000002) Force IRQL checking
    [ ] (0x00000008) Pool tracking
    [ ] (0x00000010) I/O verification
```

```
[SubKeyAddr]         [SubKeyName]
ffff960b94d779f4     PrefetchParameters
ffff960b94d77cfc     StoreParameters

 Use '!reg keyinfo ffff960b90e60000 <SubKeyAddr>' to dump the subkey details

[ValueType]          [ValueName]                 [ValueData]
REG_DWORD            ClearPageFileAtShutdown     0
REG_DWORD            DisablePagingExecutive      0
REG_DWORD            LargeSystemCache            0
REG_DWORD            NonPagedPoolQuota           0
REG_DWORD            NonPagedPoolSize            0
REG_DWORD            PagedPoolQuota              0
REG_DWORD            PagedPoolSize               0
REG_MULTI_SZ         PagingFiles                 ?:\pagefile.sys\0
REG_DWORD            SecondLevelDataCache        0
REG_DWORD            SessionPoolSize             4
REG_DWORD            SessionViewSize             30
REG_DWORD            SystemPages                 0
REG_DWORD            PhysicalAddressExtension    1
REG_DWORD            da56a5e4-287c-4a5b-86da-140a12d814cd4
REG_BINARY           PagefileUsage               0xffff960b94d77464 - d4 27 00 00 21 4a 03 00 61 80 03 00 60 cd 0
REG_DWORD            VerifyDriverLevel           100001
REG_BINARY           VerifierSettingState        0xffff960b94d76ff4 - 01 00 10 00 02 00 00 00
REG_DWORD            VerifierOptions             0
REG_SZ               VerifyDrivers               ndis.sys netmgr.sys vwifimf.sys nwifi.sys
REG_DWORD            XdvExtensionOption          0
REG_DWORD            XdvVerifierOptions          0
REG_MULTI_SZ         ExistingPageFiles           \??\C:\pagefile.sys\0
```

中断请求级别 （IRQL） 定义处理器在任何给定时间运行的硬件优先级。在 Windows 驱动程序模型中，以较高 IRQL 运行的进程将抢占以较低 IRQL 运行的线程或中断。IRQL 为 0 表示处理器正在运行正常的内核或用户模式进程。IRQL 为 1 表示处理器正在运行异步过程调用 （APC） 或页面错误。IRQL 2 用于延迟过程调用 （DPC） 和线程调度。IRQL 2 被称为 DISPATCH_LEVEL。

在 DISPATCH_LEVEL 这个级别，DPC(延迟过程) 和更低的中断被屏蔽，不能访问分页内存，所有的被访问的内存不能分页。在这个级别，能够访问的 api 大大减少。

下一步建议：

1）以管理员权限打开 cmd 命令行，运行 **verifier.exe**，暂时关闭驱动程序验证工具，减少触发驱动的潜在问题的可能。

2）需要 netmgr.sys 驱动的三方应用厂商排查其驱动，处理其对应的 IRQL 级别使用。

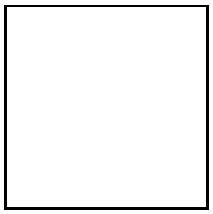
危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

神州网信 CMIT

发件人: Soul power ギ <303642690@qq.com>
发送时间: 2023 年 9 月 28 日 10:05
收件人: Wei Liang <weiliang@cmgos.com>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>

主题: 回复: 回复: [案例号: CAS-09903-Z2V6L2] % |P2|ICBC|win10 异常蓝屏需要分析 % 初次响应 CMIT:0001387

工程师，我行林总的电脑在 vpn 场景下持续蓝屏，请再次分析问题原因。



Soul power ギ
303642690@qq.com

---------- 原始邮件 ----------

发件人: "Wei Liang" <weiliang@cmgos.com>;

发送时间: 2023 年 9 月 22 日(星期五) 下午 4:17

收件人: "Soul power ギ"<303642690@qq.com>;

抄送: "ICBC_Notification"<ICBC_Notification@cmgos.com>;

主题: 回复: [案例号: CAS-09903-Z2V6L2] % |P2|ICBC|win10 异常蓝屏需要分析 % 初次响应 CMIT:0001387

许先生 您好:

感谢您的电话接听。

经过您的确认，我将归档此案例。

工单的归档并不会影响我们为您提供技术支持服务，如有其他问题，您可以随时联系我们。

案例总结：

问题定义：

用户反馈林总的设备在公网环境下连接 vpn 出现异常蓝屏问题，需要协助分析。

问题总结：

通过分析蓝屏 dump，显示 netmgr.sys 驱动触发了 DbgPrint 操作导致的蓝屏，需要 netmgr 排查其调用 DbgPrint 函数的方法。

netmgr.sys 是 TMS 的组件，需要三方应用厂商排查、处理其驱动问题。

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: 2023 年 9 月 20 日 14:45
收件人: '许翔' <303642690@qq.com>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: [案例号: CAS-09903-Z2V6L2] % |P2|ICBC|win10 异常蓝屏需要分析 % 初次响应 CMIT:0001387

许先生 您好:

分析您提供的 dump 文件，显示由于 bugcheck 代码为 **0xa**（IRQL_NOT_LESS_OR_EQUAL），这个错误检查是由使用不适当地址的内核模式设备驱动程序引起的。这个错误检查表明，在提高中断请求级别（IRQL）时，有人试图访问一个无效的地址。

发生了 0xa 的蓝屏，是由于读取了 IRQL 比较高的地址触发的。

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

IRQL_NOT_LESS_OR_EQUAL (a)
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 a kernel debugger is available get the stack backtrace.
Arguments:
Arg1: ffffac0ede2c5000, memory referenced
Arg2: 0000000000000002, IRQL
Arg3: 0000000000000000, bitfield :
      bit 0 : value 0 = read operation, 1 = write operation
      bit 3 : value 0 = not an execute operation, 1 = execute operation (only on chips which support this level of status)
Arg4: fffff8072ee4cbf7, address which referenced memory

Debugging Details:
------------------
```

查看出故障时的指令指针以及 irql 情况。

```
3: kd> ln fffff8072ee4cbf7
Browse module
Set bu breakpoint

(fffff807`2ee4c8a4)   nt!output_l+0x353   |  (fffff807`2ee4d0f4)   nt!write_char
3: kd> !irql
Debugger saved IRQL for processor 0x3 -- 2 (DISPATCH_LEVEL)
```

查看 trap frame 情况，显示访问了无效的内存地址。

```
3: kd> .trap 0xffff908a0b8a5370
NOTE: The trap frame does not contain all registers.
Some register values may be zeroed or incorrect.
rax=ffffac0ede2c5000 rbx=0000000000000000 rcx=000000007ffff812
rdx=0000000000000000 rsi=0000000000000000 rdi=0000000000000000
rip=fffff8072ee4cbf7 rsp=ffff908a0b8a5500 rbp=ffff908a0b8a5600
 r8=fffff8065ae0540f  r9=0000000000000000 r10=ffff908a0b8a57f0
r11=0000000000000000 r12=0000000000000000 r13=0000000000000000
r14=0000000000000000 r15=0000000000000000
iopl=0         nv up ei pl nz na po nc
nt!output_l+0x353:
fffff807`2ee4cbf7 443808          cmp     byte ptr [rax],r9b ds:ffffac0e`de2c5000=??
```

查看出问题时的 call stack 情况，显示 netmgr.sys 驱动触发了 DbgPrint 操作，最终导致蓝屏。

```
3: kd> knL
 # Child-SP          RetAddr           Call Site
00 ffff908a`0b8a5228 fffff807`2ee7f5e9 nt!KeBugCheckEx
01 ffff908a`0b8a5230 fffff807`2ee7b9d4 nt!KiBugCheckDispatch+0x69
02 ffff908a`0b8a5370 fffff807`2ee4cbf7 nt!KiPageFault+0x454
03 ffff908a`0b8a5500 fffff807`2ee487c7 nt!output_l+0x353
04 ffff908a`0b8a57c0 fffff807`2ee48761 nt!vsnprintf_l+0x5b
05 ffff908a`0b8a5830 fffff807`2edef213 nt!vsnprintf+0x11
06 ffff908a`0b8a5870 fffff807`2edc85fd nt!RtlStringCbVPrintfA+0x3f
07 ffff908a`0b8a58a0 fffff807`2edc84dc nt!vDbgPrintExWithPrefixInternal+0xdd
08 ffff908a`0b8a59a0 fffff806`5adfcb0d nt!DbgPrint+0x3c
09 ffff908a`0b8a59e0 fffff806`5adfd1e9 netmgr+0x1cb0d
0a ffff908a`0b8a5a60 fffff806`5adfdafc netmgr+0x1d1e9
0b ffff908a`0b8a5ac0 fffff806`5adfdc55 netmgr+0x1dafc
0c ffff908a`0b8a5b00 fffff806`5b569f57 netmgr+0x1dc55
```

查看 netmgr.sys 文件情况。

```
3: kd> lmvm netmgr
Browse full module list
start             end                 module name
fffff806`5ade0000 fffff806`5afd8000   netmgr     (no symbols)
    Loaded symbol image file: netmgr.sys
    Image path: \SystemRoot\System32\Drivers\netmgr.sys
    Image name: netmgr.sys
    Browse all global symbols  functions  data
    Timestamp:        Wed Jun  7 09:59:47 2023 (647FE493)
    CheckSum:         00033CE5
    ImageSize:        001F8000
    Translations:     0000.04b0 0000.04e4 0409.04b0 0409.04e4
    Information from resource tables:
```

该文件位置为：C:\Windows\System32\Drivers\netmgr.sys。为 2023 年 6 月版本。

对比以前的案例情况，确认**它是 TMS 的组件，需要三方应用厂商排查处理这个问题。**

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: Wei Liang
发送时间: 2023 年 9 月 19 日 17:54
收件人: 许翔 <303642690@qq.com>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: [案例号：CAS-09903-Z2V6L2] % |P2|ICBC|win10 异常蓝屏需要分析 % 初次响应 CMIT:0001387

许先生 您好:

感谢您的电话接听。

根据您提供的信息，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:

用户反馈林总的设备在公网环境下连接 vpn 出现异常蓝屏问题，需要协助分析。

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。

出现蓝屏问题的设备的 dump 文件已经下载并尝试分析，如有任何进展，会及时与您沟通，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 <weiliang@cmgos.com>
发送时间: 2023 年 9 月 19 日 17:35
收件人: 许翔 <303642690@qq.com>
抄送: Wei Liang <weiliang@cmgos.com>
主题: [案例号: CAS-09903-Z2V6L2] % |P2|ICBC|win10 异常蓝屏需要分析 % 初次响应 CMIT:0001387

许翔 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-09903-Z2V6L2 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
