吴先生 & 洪先生 你们好:

感谢电话沟通，经您的确认，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：

新设备在 V2020-L 环境下仅安装 TMS66664 版本出现蓝屏问题分析。

问题总结：

经工行与 TMS 厂商确认，authcomm.sys 出现蓝屏是一个已知问题，此案例可以关闭。

问题分析：

分析上传的 dump，查看其 call stack，显示问题的原因是 NdisRequest+0x1f 这一 frame 访问了无效的地址，而它的参数是在处理 authcomm 相关行为的时候通过 R8 传过来的。所以，问题出在 authcomm。authcomm 是 TMS 客户端相关组件，请寻求 TMS 厂商支持。

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

神州网信
CMIT

发件人: Wei Liang
发送时间: 2021 年 9 月 16 日 17:50
收件人: 吴毓杰 <win10sup@sdc.icbc.com.cn>; 'hongbo@icbc.com.cn' <hongbo@icbc.com.cn>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: [案例号: CAS-04791-T4Z7M1] % |P3|ICBC|总行新设备 V2020-L 系统蓝屏分析 % 初次响应 CMIT:0001289

吴先生 & 洪先生 你们好:

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:

新设备在 V2020-L 环境下仅安装 TMS66664 版本出现蓝屏问题分析。

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。

分析上传的日志，BugCheck 报错为 d1，这表明内核模式驱动程序在进程 IRQL 过高时尝试访问可分页内存。

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

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: 0000000000000000, memory referenced
Arg2: 0000000000000002, IRQL
Arg3: 0000000000000008, value 0 = read operation, 1 = write operation
Arg4: 0000000000000000, address which referenced memory

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

BUGCHECK_CODE:  d1

BUGCHECK_P1: 0

BUGCHECK_P2: 2

BUGCHECK_P3: 8

BUGCHECK_P4: 0

READ_ADDRESS:  0000000000000000

PROCESS_NAME:  scauth.exe
```

查看当前的 callstack 显示访问了 0 地址。

```
6: kd> .trap 0xffffb602da0b7360
NOTE: The trap frame does not contain all registers.
Some register values may be zeroed or incorrect.
rax=0000000000000000 rbx=0000000000000000 rcx=ffff8b0df397b920
rdx=ffff8b0df47f4360 rsi=0000000000000000 rdi=0000000000000000
rip=0000000000000000 rsp=ffffb602da0b74f8 rbp=0000000000000800
 r8=ffff8b0df47f4360  r9=ffff8b0df397b920 r10=0000000000000002
r11=ffffb602da0b7500 r12=0000000000000000 r13=0000000000000000
r14=0000000000000000 r15=0000000000000000
iopl=0         nv up ei ng nz na po nc
00000000`00000000 ??              ???
6: kd> k
  *** Stack trace for last set context - .thread/.cxr resets it
 # Child-SP          RetAddr           Call Site
00 ffffb602`da0b74f8 fffff807`592dedaf 0x0
01 ffffb602`da0b7500 fffff807`58c82a95 ndis!NdisRequest+0x1f
02 ffffb602`da0b7530 fffff807`58c819f8 authcomm+0x2a95
03 ffffb602`da0b7560 fffff807`58c821f6 authcomm+0x19f8
04 ffffb602`da0b7590 fffff807`58c81369 authcomm+0x21f6
05 ffffb602`da0b7630 fffff807`58c820d9 authcomm+0x1369
06 ffffb602`da0b76a0 fffff807`52529059 authcomm+0x20d9
07 ffffb602`da0b76f0 fffff807`52a925c1 nt!IofCallDriver+0x59
08 ffffb602`da0b7730 fffff807`52a6ce3c nt!IopSynchronousServiceTail+0x1b1
09 ffffb602`da0b77e0 fffff807`52a130e6 nt!IopXxxControlFile+0xe0c
0a ffffb602`da0b7920 fffff807`525e7d05 nt!NtDeviceIoControlFile+0x56
0b ffffb602`da0b7990 00000000`77801cbc nt!KiSystemServiceCopyEnd+0x25
0c 00000000`0221efb8 00000000`00000000 0x77801cbc
```

查看具体的 frame 的细节。

```
6: kd> .frame /r 01
01 ffffb602`da0b7500 fffff807`58c82a95 ndis!NdisRequest+0x1f
rax=0000000000000000 rbx=0000000000000000 rcx=ffff8b0df397b920
rdx=ffff8b0df47f4360 rsi=0000000000000000 rdi=0000000000000000
rip=fffff807592dedaf rsp=ffffb602da0b7500 rbp=0000000000000800
 r8=ffff8b0df47f4360  r9=ffff8b0df397b920 r10=0000000000000002
r11=ffffb602da0b7500 r12=0000000000000000 r13=0000000000000000
r14=0000000000000000 r15=0000000000000000
iopl=0         nv up ei ng nz na po nc
cs=0010  ss=0018  ds=0000  es=0000  fs=0000  gs=0000             efl=00010286
ndis!NdisRequest+0x1f:
fffff807`592dedaf 8903            mov     dword ptr [rbx],eax ds:00000000`00000000=????????
6: kd> ub fffff807`58c82a95
authcomm+0x2a75:
fffff807`58c82a75 894320          mov     dword ptr [rbx+20h],eax
fffff807`58c82a78 488d573c        lea     rdx,[rdi+3Ch]
fffff807`58c82a7c 488d4c2438      lea     rcx,[rsp+38h]
fffff807`58c82a81 48895330        mov     qword ptr [rbx+30h],rdx
fffff807`58c82a85 488b17          mov     rdx,qword ptr [rdi]
fffff807`58c82a88 4c8bc3          mov     r8,rbx
fffff807`58c82a8b 89442438        mov     dword ptr [rsp+38h],eax
fffff807`58c82a8f ff15d3150000    call    qword ptr [authcomm+0x4068 (fffff807`58c84068)]
6: kd> dq ffff8b0df47f4360
ffff8b0d`f47f4360  00000000`00000000 00000000`00000000
ffff8b0d`f47f4370  00000000`00000000 00000000`00000000
ffff8b0d`f47f4380  00000000`00000000 00000000`01010102
ffff8b0d`f47f4390  ffff8b0d`f1a3ed3c 00000000`00000006
ffff8b0d`f47f43a0  00000000`00000000 00000000`00000000
ffff8b0d`f47f43b0  00000000`00000000 00000000`00000000
ffff8b0d`f47f43c0  00000000`00000000 00000000`00000000
ffff8b0d`f47f43d0  00000000`00000000 00000000`00000000
```

问题的原因是 NdisRequest+0x1f 这一 frame 访问了无效的地址，而它的参数是在处理 **authcomm** 相关行为的时候通过 R8 传过来的。所以，问题出在 **authcomm**。

查看 authcomm 组件情况：

```
6: kd> lmvm authcomm
Browse full module list
start             end                 module name
fffff807`58c80000 fffff807`58c88000   authcomm   (no symbols)
    Loaded symbol image file: authcomm.sys
    Image path: \SystemRoot\system32\drivers\authcomm.sys
    Image name: authcomm.sys
    Browse all global symbols  functions  data
    Timestamp:        Wed Jun 16 22:15:45 2021 (60CA0791)
    CheckSum:         0000EA5C
    ImageSize:        00008000
    Translations:     0000.04b0 0000.04e4 0409.04b0 0409.04e4
    Information from resource tables:
```

此次蓝屏原因出在 authcomm.sys 驱动，相关的 dump 分析与以前的蓝屏案例一样，经过您的确认，这个驱动属于 TMS 客户端。

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: 2021 年 9 月 16 日 16:51
收件人: 吴毓杰 <win10sup@sdc.icbc.com.cn>
抄送: Wei Liang <weiliang@cmgos.com>
主题: [案例号: CAS-04791-T4Z7M1] % |P3|ICBC|总行新设备 V2020-L 系统蓝屏分析 % 初次响应 CMIT:0001289

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-04791-T4Z7M1 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
