

洪先生 & 吴先生 你们好:

根据刚才的电话沟通, 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:

Windows 10 神州网信政府版 V2020-L 系统蓝屏。

问题总结:

从 dump 中分析与 vwifimf 组件有关, 此组件属于 TMS 客户端, 用户升级 TMS 客户端查看后续运行情况。

问题分析:

分析上传的 dump, 查看其 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。

查看与此数据包有关的 pool, 提示 Filt 异常, 其所有者为 vwifimf.sys, 是 TMS 客户端相关组件, 与以前处理的有关 TMS 的 vwifimf 案例一样, 建议升级 TMS 客户端。

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 9 月 13 日 10:22

收件人: '吴毓杰' <win10sup@sdicbc.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-04760-M8H3C4] % |P3|ICBC|总行 win10 神州网信政府版 V2020-L 系统蓝屏分析 % 初次响应 CMIT:0001187

洪先生 & 吴先生 你们好:

总行 Windows 10 神州网信政府版 V2020-L 系统, 9 月 9 号上传的蓝屏日志详细分析如下:

dump 的 bugcheck code 为 0xd1, 指的是在当前 IRQL 较高的情况下(DISPATCH_LEVEL=2)去访问了一个无效的内存地址, 导致机器蓝屏。

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。

```
0: kd> k
# Child-SP          RetAddr          Call Site
00 fffff806`28080e98 fffff806`254782e9 nt!KeBugCheckEx
01 fffff806`28080ea0 fffff806`254746d4 nt!KiBugCheckDispatch+0x69
02 fffff806`28080fe0 fffff806`329394fd nt!KiPageFault+0x454
03 fffff806`28081170 fffff806`3293d66d nwifi!Dot11SendCompletion+0x35
04 fffff806`280811b0 fffff806`2b886a13 nwifi!Pt6SendComplete+0x1d
05 fffff806`280811e0 fffff806`2b881efd ndis!NdisCallSendCompleteHandler+0x33
06 fffff806`28081220 fffff806`3082593d ndis!NdisMSendNetBufferListsComplete+0x26d
07 fffff806`28081330 fffff806`307f2ef0 wdiwifi!CPort::SendCompleteNetBufferLists+0xf5
08 fffff806`28081380 fffff806`307e74da wdiwifi!CAdapter::SendCompleteNbl+0x11c
09 fffff806`280813f0 fffff806`307e71f1 wdiwifi!CTxMgr::CompleteNdisNbl+0xbe
0a fffff806`28081450 fffff806`307e4395 wdiwifi!CTxMgr::CompleteNBLS+0x59
0b fffff806`28081490 fffff806`307d7440 wdiwifi!CTxMgr::TxTransferCompleteInd+0x5c9
0c fffff806`28081550 fffff806`2ff1d388 wdiwifi!AdapterTxTransferCompleteInd+0x10
0d fffff806`28081580 fffff806`2ff6db06 Netwtw10+0x4d388
0e fffff806`280815e0 fffff806`302ed062 Netwtw10+0x9db06
0f fffff806`28081710 fffff806`302fb181 Netwtw10+0x41d062
10 fffff806`28081750 fffff806`3031ff8b Netwtw10+0x42b181
11 fffff806`280817e0 fffff806`302f1b32 Netwtw10+0x44ff8b
12 fffff806`28081940 fffff806`302e9133 Netwtw10+0x421b32
13 fffff806`28081a30 fffff806`302e79a8 Netwtw10+0x419133
14 fffff806`28081a90 fffff806`302e8a8b Netwtw10+0x4179a8
15 fffff806`28081b00 fffff806`2b886ba8 Netwtw10+0x418a8b
0: kd> .frame /r 0x3
03 fffff806`28081170 fffff806`3293d66d nwifi!Dot11SendCompletion+0x35
rax=0000000000000000 rbx=fffffffffffffffe8 rcx=ffffe70ed64f95b0
rdx=ffffe70edff52640 rsi=ffffe70edff52640 rdi=ffffe70ed64f95f0
rip=fffff806329394fd rsp=fffff80628081170 rbp=0000000000000000
r8=0000000000000000 r9=0000000000000000 r10=0000000000000001
r11=fffff80628081050 r12=ffffe70ecc3659a0 r13=ffffe70ecc2b5020
r14=ffffe70ecc364058 r15=ffffe70ecc367080
iopl=0         nv up ei ng nz na po nc
cs=0010  ss=0000  ds=002b  es=002b  fs=0053  gs=002b             efl=00000286
nwifi!Dot11SendCompletion+0x35:
fffff806`329394fd 48b03          mov     rax,qword ptr [rbx]
ds:002b:ffffffffff`fffffe8=????????????????
```

查看其数据包结构

```

0: kd> dt fffff70edff52640 nwifi!_NET_BUFFER_LIST
+0x000 Next : (null)
+0x008 FirstNetBuffer : 0xfffff70e`dff527c0 _NET_BUFFER
+0x000 Link : _SLIST_HEADER
+0x000 NetBufferListHeader : _NET_BUFFER_LIST_HEADER
+0x010 Context : 0xfffff70e`d64f95b0 _NET_BUFFER_LIST_CONTEXT
+0x018 ParentNetBufferList : (null)
+0x020 NdisPoolHandle : 0xfffff70e`cc364380 Void
+0x030 NdisReserved : [2] (null)
+0x040 ProtocolReserved : [4] 0xfffff70e`e29a4a30 Void
+0x060 MiniportReserved : [2] (null)
+0x070 Scratch : (null)
+0x078 SourceHandle : 0xfffff70e`cc361a20 Void
+0x080 NblFlags : 0
+0x084 ChildRefCount : 0n0
+0x088 Flags : 0x500
+0x08c Status : 0n0
+0x08c NdisReserved2 : 0
+0x090 NetBufferListInfo : [26] (null)

```

查看其 pool 情况，显示 Filt tag 有问题。

```

0: kd> !pool 0xfffff70e`cc364380
Pool page fffff70ecc364380 region is Nonpaged pool
fffff70ecc364000 size: 350 previous size: 0 (Allocated) ND
*fffff70ecc364360 size: a00 previous size: 0 (Allocated) *Filt
Owning component : Unknown (update pooltag.txt)
fffff70ecc364d70 size: 200 previous size: 0 (Allocated) Irp
fffff70ecc364f70 size: 70 previous size: 0 (Free) ..y.

```

查看其 tag 属于 vwifimf.sys，其属于 TMS 客户端相关组件，与以前处理的有关 TMS 的 vwifimf 案例一样，建议升级 TMS 客户端。

```

0: kd> !mex.tag Filt
Mex External 3.0.0.7172 Loaded!
Name      Number of Hits Version Time Stamp      Location
=====
vwifimf      1 0.0.0.0 03/24/2021 01:06:44 \SystemRoot\system32\DRIVERS\vwifimf.sys

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

0: kd> lmvm vwifimf
Browse full module list
start      end      module name
fffff806`2cab0000 fffff806`2caba000 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: Wed Mar 24 09:06:44 2021 (605A90A4)
Checksum: 000069CA
ImageSize: 0000A000
Translations: 0000.04b0 0000.04e4 0409.04b0 0409.04e4
Information from resource tables:

```

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 9 月 9 日 16:57

收件人: 吴毓杰 <win10sup@cdc.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-04760-M8H3C4] % |P3|ICBC|总行 win10 神州网信政府版 V2020-L 系统蓝屏分析 % 初次响应 CMIT:0001187

洪先生 & 吴先生 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:

Windows 10 神州网信政府版 V2020-L 系统蓝屏。

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。

初步分析您上传的日志, 提示 BugCheck 为 D1, 且当前出错的进程为 scclient.exe

```

BUGCHECK_CODE: d1
BUGCHECK_P1: ffffffff80000000
BUGCHECK_P2: 2
BUGCHECK_P3: 0
BUGCHECK_P4: fffff806329394fd
READ_ADDRESS: ffffffff80000000
PROCESS_NAME: scclient.exe
DPC_STACK_BASE: fffff80628081fb0

TRAP_FRAME: fffff80628080fe0 -- (.trap 0xffff80628080fe0)
NOTE: The trap frame does not contain all registers.
Some register values may be zeroed or incorrect.
rax=0000000000000000 rbx=0000000000000000 rcx=ffffe70ed64f95b0
rdx=ffffe70edf52640 rsi=0000000000000000 rdi=0000000000000000
rip=fffff806329394fd rsp=fffff80628081170 rbp=0000000000000000
r8=0000000000000000 r9=0000000000000000 r10=0000000000000001
r11=fffff80628081050 r12=0000000000000000 r13=0000000000000000
r14=0000000000000000 r15=0000000000000000
iopl=0         nv up ei pl nz na pe nc
nwifi!Dot11SendCompletion+0x35:  mov     rax,qword ptr [rbx] ds:00000000`00000000=????????????
fffff806`329394fd 488b03  Resetting default scope

```

scclient.exe 应用属于 TMS 客户端，当前 TMS 客户端版本为 66621 版本。

这个问题与前期处理过的蓝屏问题类似，与 TMS 客户端有关，建议您升级 TMS 客户端版本，测试是否还复现问题。

我这边会进一步分析当前 dump，相关分析情况会及时与你们沟通。

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 9 日 16:17
收件人: 吴毓杰 <win10sup@sdic.icbc.com.cn>
抄送: Wei Liang <weiliang@cmgos.com>
主题: [案例号: CAS-04760-M8H3C4] % |P3|ICBC|总行 win10 神州网信政府版 V2020-L 系统蓝屏分析 % 初次响应 CMIT:0001187

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-04760-M8H3C4 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”。