Hi All:

关于 vwifimf.sys 导致系统蓝屏的问题，神州网信与工行一直以来保持紧密沟通，蓝屏 dump 的详细分析结果会第一时间发送给工行同事，本次的分析主要围绕案例：**CAS-05796-S4W5H4** 进行，请查看附件邮件获取全部的详细信息，在此不再详述。

目前仅凭蓝屏 dump 的结果记录，操作系统层面是无法分析过滤驱动内部的处理过程。需要 TMS 的大力配合为 vwifimf.sys 驱动增加跟踪调试日志，对 NBL 引发蓝屏前的处理过程进行记录。增加跟踪调试日志的需求在 3 月 29 日提出，至今未收到符合神州网信要求的调试日志（4 月 26 日收到的日志中时间戳与蓝屏时间不对应，不具备参考价值），为了帮助工行用户尽早摆脱蓝屏问题的困扰，请 TMS 方按以下要求提供调试日志，谢谢!

具体调试要求如下:

1、固定一台频繁复现蓝屏的电脑，TMS 在其软件内部增加调试手段及记录。

2、请 TMS 跟踪 vwifimf 内部对 NBL 的处理过程，调试跟踪其 FilterSendNetBufferListsComplete 函数入参及函数内部的相关变量值，记录 SendNetBufferListsCompleteHandler 处理 NBL 时的相关参数信息。

3、待 TMS 按以上要求成功获取对应调试日志后，神州网信协助分析与调试日志同一时间生成的蓝屏 dump 文件。

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

神州网信
CMIT

发件人: Windows Server 技术支持 <windowsserversupport@sdc.icbc.com.cn>
发送时间: 2022 年 5 月 23 日 10:58

收件人: Li Qi <liqi@cmgos.com>
抄送: 李粤 <liyue@sdc.icbc.com.cn>; 吴毓杰 <555016231@sdc.com>; Liu Jian <liujian@cmgos.com>; zhangjiou <zhangjiou@360.cn>; songshijie1 <songshijie1@360.cn>; yangshijian <yangshijian@360.cn>; liyan16 <liyan16@360.cn>; liyeshaung <liyeshaung@360.cn>; win10 升级支持 <win10sup@sdc.icbc.com.cn>; 徐健鸿 <555100412@sdc.com>; Windows Server 技术支持 <windowsserversupport@sdc.icbc.com.cn>; ICBC_Notification <ICBC_Notification@cmgos.com>; Wei Liang <weiliang@cmgos.com>
主题: 回复:【外来邮件，注意核实】回复: [案例号: CAS-06133-X9Z4Q7] % |P2|ICBC|软件开发中心政府版系统异常蓝屏问题 % 初次响应 CMIT:0001362

关于 TMS 提出的问题，请神州网信工程看一下。请两边厂商密切联系，并尽快分析出问题所在给出相关解决方案。

-----原始邮件-----

发件人: "李响" <lixiang11@360.cn>
发送时间: 2022-05-21 17:08:04
收件人: "客户端管理系统" <客户端管理系统.软件开发中心系统一部@工商银行.icbc>,"win10 升级支持" <win10 升级支持.软件开发中心系统一部@工商银行.icbc>
抄送: "陈锦祥" <陈锦祥.软件开发中心系统一部@工商银行.icbc>,"李粤" <李粤.软件开发中心系统一部@工商银行.icbc>,"李汇腾" <李汇腾.软件开发中心系统一部@工商银行.icbc>,"张际鸥" <zhangjiou@360.cn>,"曹羽" <caoyu5@360.cn>,"李业双" <liyeshuang@360.cn>,"宋仕杰" <songshijie1@360.cn>
主题: 【外来邮件，注意核实】答复: 软开中心政府版系统异常蓝屏 TMS 厂商通软方面暂无进展

vwifimf 驱动已经两年没有任何改动，此问题非 TMS 问题，已经多次回复确认，为了配合调查 5.1 前将我们 vwifimf 私有符号文件给操作系统端，截止目前并未反馈任何分析结果。

李响
终端安全产品事业部
360 政企安全集团

手机：18624336057
邮件：lixiang11@360.cn
地址：沈阳市浑南区文汇街 19 号（金鹏龙高科技园）21 号楼

☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆

中国工商银行软件开发中心（珠海）
许 翔
系统一部
电话：17606669571

☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆

-----原始邮件-----

发件人： "Li Qi" <liqi@cmgos.com>
发送时间： 2022-05-06 11:41:41
收件人： "Windows Server 技术支持" <windowsserver 技术支持.软件开发中心系统一部@工商银行.icbc>
抄送： "ICBC_Notification" <icbc_notification@cmgos.com>,"win10 升级支持" <win10 升级支持.软件开发中心系统一部@工商银行.icbc>
主题： 【外来邮件，注意核实】回复：［案例号：CAS-06133-X9Z4Q7 ］ %|P2|ICBC|软件开发中心政府版系统异常蓝屏问题 % 初次响应 CMIT:0001362

许先生，您好：

TMS 提供的分析报告在大概两年前最初发现 NBL 蓝屏问题的时候就已经这样说明了（历史沟通可参见附件 1）。之后 TMS 进行过几次软件更新，问题得以缓解。今年该问题再次出现，再次讨论此问题的目的是希望可以明确在 TMS 和神州网信两方的能力范围内进行进一步排查。这里所谓的进一步排查是指针对一次明确的蓝屏事件，TMS 可以进行断点调试，来证明确实如产品流程设计所言，对问题 NBL 进行了过滤处理。而从 dump 上的已知信息来看，并不是 TMS 所指出的重组数据包由自身的 SendNetBufferListsCompleteHandler 中来进行释放，而是交给 NdisFSendNetBufferListsComplete。

因为 dump 是蓝屏时的内存信息记录，尽管我们在之前的分析中也尝试过很多方式进行 vwifimf 的跟踪，包括使用 TMS 提供的 private symbol 也并没有从操作系统的层面解析到引发蓝屏的 NBL 的 SourceHandle 和 FilterHandle 的动态过程信息。因此无法证明在需要重组的 NBL 创建之初，“调用 SendNetBufferListsHandler 发送数据包时，会将 SourceHandle 设置成与 FilterHandle 值”。这也是我们在之前希望 TMS 可以进行断点调试的原因。这样可以自证 vwifimf 的逻辑处理是否与流程图一致。在 TMS 之前提供的一份调试日志中，其结果是晚于 dump 生成时间的，并没有记录引发蓝屏的 NBL 相关参数。无法与流程图所述进行比对，对当前的问题分析并没有帮助（具体可参见附件 2）。因此需要 TMS 增加调试手段对 NBL 引发蓝屏前的处理过程进行记录，没有 TMS 的日志信息，仅凭 dump 的结果记录，操作系统层面是无法分析过滤驱动内部的处理过程的。

因此我们的建议是：

1. 固定一台频繁复现蓝屏的电脑，TMS 在其软件内部增加调试手段及记录。
2. 结合 TMS 给出的流程图， 跟踪 vwifimf 内部对 NBL 的处理过程，调试跟踪其 FilterSendNetBufferListsComplete 函数入参及函数内部的相关变量值，记录 SendNetBufferListsCompleteHandler 处理 NBL 时的相关参数信息。
3. 待成功抓取后，我们可以以 dump 内容从操作系统层面进行辅助验证。

李琦 Li Qi
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话： 4008180055
电子邮箱 Email: liqi@cmgos.com

发件人: Windows Server 技术支持 <windowsserversupport@sdc.icbc.com.cn>
发送时间: 2022 年 5 月 5 日 17:36
收件人: Li Qi <liqi@cmgos.com>
抄送: Windows Server 技术支持 <windowsserversupport@sdc.icbc.com.cn>; ICBC_Notification <ICBC_Notification@cmgos.com>; win10 升级支持 <win10sup@sdc.icbc.com.cn>

主题: 回复:【外来邮件，注意核实】回复: [案例号: CAS-06133-X9Z4Q7] % |P2|ICBC|软件开发中心政府版系统异常蓝屏问题 % 初次响应 CMIT:0001362

通软公司根据蓝屏机器 dump 给出如下分析报告，请操作系统参考并协助排查。谢谢。

vwifimf.sys 是一个过滤驱动，主要作用就是处理无线 802.1x 数据包，所以每个 802.1x 相关数据包都会经过 vwifimf 驱动，表现为由 vwifimf 申请的内存，所以查看到数据包的内存是由 vwifimf.sys 申请，这是正常现象。

产品通过 NdisFRegisterFilterDriver 中的 SendNetBufferListsHandler（开始发送数据包函数）和 SendNetBufferListsCompleteHandler（发送完成数据包函数）来实现 802.1x 数据包的发送。主要有两种场景需要处理，一个是我们关心的 802.1x 数据包场景，需要重组数据包，另一个是其他数据包场景，程序直接转发，不做任何多余处理。

其他数据包场景，程序会按照标准的方式由 SendNetBufferListsHandler 调用 NdisFSendNetBufferLists 向下层驱动转发处理，完成后再由 SendNetBufferListsCompleteHandler 调用 NdisFSendNetBufferListsComplete 向上层驱动转发处理。

需要重组 802.1x 数据包场景，程序会在 SendNetBufferListsHandler 接口中，针对原始的 NBL，直接调用 NdisFSendNetBufferListsComplete 完成请求。然后分配一段内存，重组 NBL 请求。新重组的 NBL 会设置 SourceHandle 等字段，用于标识是否为重组数据包，并调用 NdisFSendNetBufferLists 转发给下层驱动。完成后会在 SendNetBufferListsCompleteHandler 中释放重组的 NBL，并且不会再调用 NdisFSendNetBufferListsComplete 向上层驱动转发处理。

从 dump 信息看，该数据包为需要重组的数据包，程序在调用 SendNetBufferListsHandler 发送数据包时，会将 SourceHandle 设置成与 FilterHandle 值一样。现在发现在系统回调 SendNetBufferListsCompleteHandler 之后，SourceHandle 和 FilterHandle 的值就不一样了，导致系统崩溃。怀疑是被其他驱动修改或破坏导致的。

TMS 端能看到的信息有限，我们将符号文件提供，请操作系统帮忙排查，SourceHandle 和 FilterHandle 值不一样的原因。

☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆

中国工商银行软件开发中心（珠海）

许 翔
系统一部
电话：17606669571
☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆

-----原始邮件-----

发件人： "Li Qi" <liqi@cmgos.com>
发送时间： 2022-04-29 17:01:54
收件人： "Windows Server 技术支持" <windowsserver 技术支持.软件开发中心系统一部@工商银行.icbc>
抄送： "ICBC_Notification" <icbc_notification@cmgos.com>,"win10 升级支持" <win10 升级支持.软件开发中心系统一部@工商银行.icbc>
主题： 【外来邮件，注意核实】回复：［案例号：CAS-06133-X9Z4Q7 ］ %|P2|ICBC|软件开发中心政府版系统异常蓝屏问题 % 初次响应 CMIT:0001362

许先生，您好:

如刚才电话沟通，经您的确认，此 case 将暂做关闭处理，以下为案例总结，请您知悉:

Case No：CAS-06133-X9Z4Q7

问题描述：

==========

用户反馈软件开发中心出现 2 台电脑出现偶发性蓝屏，已上传相关 dump 日志。

问题分析：

==========

用户上传两个 dump 已分析完毕，其中 NBL 问题由 case：CAS-05796-S4W5H4 继续跟踪处理；另外华为云桌面在处理 IRP 相关操作时的策略管控问题已进行相关修改，蓝屏问题不再复现。

问题总结：

==========

经用户确认，目前问题已解决，暂无其他问题，可关闭此 case。

以上，如您后续有任何问题，可随时与我们联系，谢谢。

李琦 Li Qi
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话： 4008180055
电子邮箱 Email: liqi@cmgos.com

发件人: Li Qi
发送时间: 2022 年 4 月 28 日 11:39
收件人: '许翔' <windowsserversupport@sdc.icbc.com.cn>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>; 'win10 升级支持' <win10sup@sdc.icbc.com.cn>
主题: 回复: [案例号: CAS-06133-X9Z4Q7] % |P2|ICBC|软件开发中心政府版系统异常蓝屏问题 % 初次响应 CMIT:0001362

许先生，您好:

您提供的两个 dump 分析如下，供您参考:

liyue-hwclient.DMP：

该 dump bugcheck 为 7f，其中参数 1 为。表明在调用先前异常的处理程序期间发生异常。通常，这两个异常是串行处理的。但是，有几个异常不能串行处理，在这种情况下，处理器会发出双重故障信号。双重故障有两个常见原因： 1. 内核堆栈溢出。当一个保护页面被命中并且内核试图推送一个陷阱帧时，就会发生这种溢出。由于没有剩余堆栈，导致堆栈溢出，导致双重故障。2. 另一个常见原因是硬件问题。

```
UNEXPECTED_KERNEL_MODE_TRAP (7f)
This means a trap occurred in kernel mode, and it's a trap of a kind
that the kernel isn't allowed to have/catch (bound trap) or that
is always instant death (double fault).  The first number in the
bugcheck params is the number of the trap (8 = double fault, etc)
Consult an Intel x86 family manual to learn more about what these
traps are. Here is a *portion* of those codes:
If kv shows a taskGate
        use .tss on the part before the colon, then kv.
Else if kv shows a trapframe
        use .trap on that value
Else
        .trap on the appropriate frame will show where the trap was taken
        (on x86, this will be the ebp that goes with the procedure KiTrap)
Endif
kb will then show the corrected stack.
Arguments:
Arg1: 0000000000000008, EXCEPTION_DOUBLE_FAULT
Arg2: fffff8034e28ae50
Arg3: ffffac8644e80fd0
Arg4: fffff803496dccae
```

其对应的陷阱帧如下：

0: kd> .trap 0xfffff8034e28ae50

NOTE: The trap frame does not contain all registers.

Some register values may be zeroed or incorrect.

rax=fffff803496e1960 rbx=0000000000000000 rcx=ffffac8644e81000

rdx=fffff803496e1960 rsi=0000000000000000 rdi=0000000000000000

rip=fffff803496dccae rsp=ffffac8644e80fd0 rbp=0000000000000000

r8=0000000000000000 r9=ffffac8644e81568 r10=0000000000000000

r11=0000000000000000 r12=0000000000000000 r13=0000000000000000

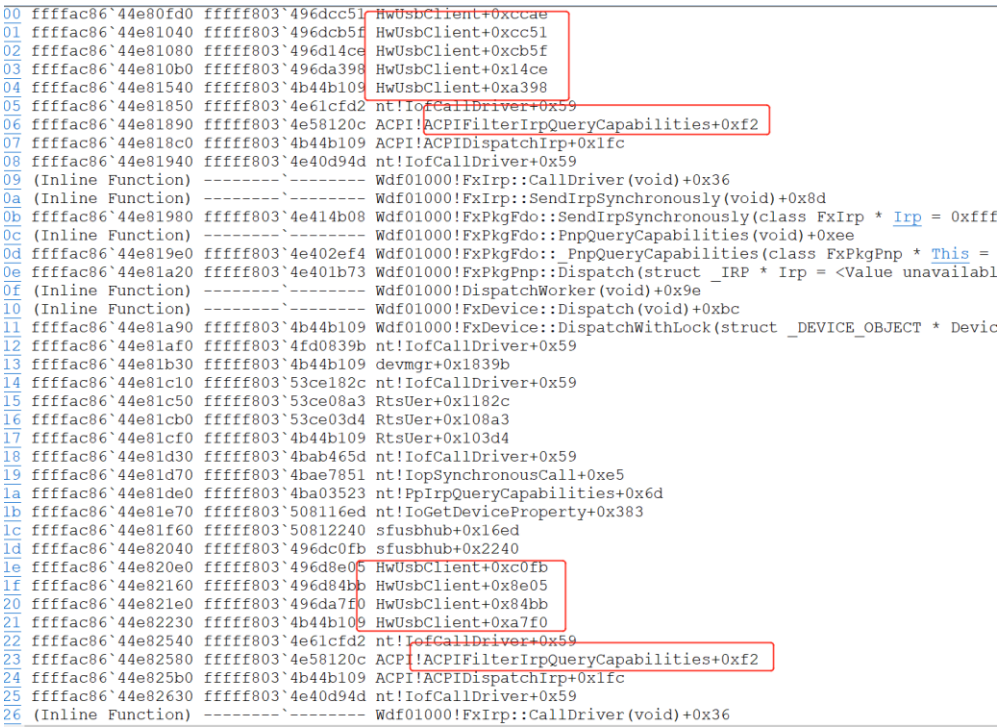
r14=0000000000000000 r15=0000000000000000

iopl=0   nv up ei ng nz na po cy

HwUsbClient+0xccae:

fffff803`496dccae e84d010000      call    HwUsbClient+0xce00 (fffff803`496dce00)

也就是说 HwUsbClient 在进行 USB 的 irp query 时触发陷阱，造成内存溢出，这是蓝屏的直接原因。那么为什么 HwUsbClient 会触发陷阱呢，通过 call stack 的查询，可以看到在进行 IRP 操作时一直在循环尝试，进入 lock。这是不正常的，也导致内存堆栈的不断增加。



```
00 ffffac86`44e80fd0 fffff803`496dcc51 HwUsbClient+0xccae
01 ffffac86`44e81040 fffff803`496dcb5f HwUsbClient+0xcc51
02 ffffac86`44e81080 fffff803`496d14ce HwUsbClient+0xcb5f
03 ffffac86`44e810b0 fffff803`496da398 HwUsbClient+0x14ce
04 ffffac86`44e81540 fffff803`4b44b109 HwUsbClient+0xa398
05 ffffac86`44e81850 fffff803`4e61cfd2 nt!IofCallDriver+0x59
06 ffffac86`44e81890 fffff803`4e58120c ACPI!ACPIFilterIrpQueryCapabilities+0xf2
07 ffffac86`44e818c0 fffff803`4b44b109 ACPI!ACPIDispatchIrp+0x1fc
08 ffffac86`44e81940 fffff803`4e40d94d nt!IofCallDriver+0x59
09 (Inline Function) --------`-------- Wdf01000!FxIrp::CallDriver(void)+0x36
0a (Inline Function) --------`-------- Wdf01000!FxIrp::SendIrpSynchronously(void)+0x8d
0b ffffac86`44e81980 fffff803`4e414b08 Wdf01000!FxPkgFdo::SendIrpSynchronously(class FxIrp * Irp = 0xfff
0c (Inline Function) --------`-------- Wdf01000!FxPkgFdo::PnpQueryCapabilities(void)+0xee
0d ffffac86`44e819e0 fffff803`4e402ef4 Wdf01000!FxPkgFdo::_PnpQueryCapabilities(class FxPkgPnp * This =
0e ffffac86`44e81a20 fffff803`4e401b73 Wdf01000!FxPkgPnp::Dispatch(struct _IRP * Irp = <Value unavailabl
0f (Inline Function) --------`-------- Wdf01000!DispatchWorker(void)+0x9e
10 (Inline Function) --------`-------- Wdf01000!FxDevice::Dispatch(void)+0xbc
11 ffffac86`44e81a90 fffff803`4b44b109 Wdf01000!FxDevice::DispatchWithLock(struct _DEVICE_OBJECT * Devic
12 ffffac86`44e81af0 fffff803`4fd0839b nt!IofCallDriver+0x59
13 ffffac86`44e81b30 fffff803`4b44b109 devmgr+0x1839b
14 ffffac86`44e81c10 fffff803`53ce182c nt!IofCallDriver+0x59
15 ffffac86`44e81c50 fffff803`53ce08a3 RtsUer+0x1182c
16 ffffac86`44e81cb0 fffff803`53ce03d4 RtsUer+0x108a3
17 ffffac86`44e81cf0 fffff803`4b44b109 RtsUer+0x103d4
18 ffffac86`44e81d30 fffff803`4bab465d nt!IofCallDriver+0x59
19 ffffac86`44e81d70 fffff803`4bae7851 nt!IopSynchronousCall+0xe5
1a ffffac86`44e81de0 fffff803`4ba03523 nt!PpIrpQueryCapabilities+0x6d
1b ffffac86`44e81e70 fffff803`508116ed nt!IoGetDeviceProperty+0x383
1c ffffac86`44e81f60 fffff803`50812240 sfusbhub+0x16ed
1d ffffac86`44e82040 fffff803`496dc0fb sfusbhub+0x2240
1e ffffac86`44e820e0 fffff803`496d8e05 HwUsbClient+0xc0fb
1f ffffac86`44e82160 fffff803`496d84bb HwUsbClient+0x8e05
20 ffffac86`44e821e0 fffff803`496da7f0 HwUsbClient+0x84bb
21 ffffac86`44e82230 fffff803`4b44b109 HwUsbClient+0xa7f0
22 ffffac86`44e82540 fffff803`4e61cfd2 nt!IofCallDriver+0x59
23 ffffac86`44e82580 fffff803`4e58120c ACPI!ACPIFilterIrpQueryCapabilities+0xf2
24 ffffac86`44e825b0 fffff803`4b44b109 ACPI!ACPIDispatchIrp+0x1fc
25 ffffac86`44e82630 fffff803`4e40d94d nt!IofCallDriver+0x59
26 (Inline Function) --------`-------- Wdf01000!FxIrp::CallDriver(void)+0x36
```

以下为 HwClient 的版本：

0: kd> lmvm HwUsbClient

Browse full module list

start end module name

fffff803`496d0000 fffff803`496f4000 HwUsbClient (no symbols)

Loaded symbol image file: HwUsbClient.sys

Image path: \SystemRoot\system32\drivers\HwUsbClient.sys

Image name: HwUsbClient.sys

Browse all global symbols functions data

Timestamp: Fri Sep 18 10:00:57 2020 (5F6414D9)

CheckSum: 00021C97

ImageSize: 00024000

Translations: 0000.04b0 0000.04e4 0409.04b0 0409.04e4

下一步动作：

请检查是否有 HwUsbClient 的更新版本，可以尝试更新。由于此次蓝屏是 double fault 问题，因此请尝试插拔发生蓝屏时的 USB 设备，观察是否问题可以稳定复现，如仅为偶发问题，可暂时忽略。

MEMORY TMS lanping.DMP：

该 dump bugcheck 为 0xD1，与正在处理的 TMS 问题一致，由于 vwifimf filter driver 没有完成并释放由自身创建的 NBL- ffff888b05519da0，将其传给 nwifi 导致错误蓝屏。以下为部分 dump 截图：

```
0: kd> kpL
 # Child-SP          RetAddr           Call Site
00 fffff803`5426e338 fffff803`51224069 nt!KeBugCheckEx
01 fffff803`5426e340 fffff803`51220369 nt!KiBugCheckDispatch+0x69
02 fffff803`5426e480 fffff803`5406a5b5 nt!KiPageFault+0x469
03 fffff803`5426e610 fffff803`5406e6ed nwifi!Dot11SendCompletion+0x35
04 fffff803`5426e650 fffff803`524239b5 nwifi!Pt6SendComplete+0x1d
05 fffff803`5426e680 fffff803`53262adb VerifierExt!XdvNdisFilterSendNetBufferListsCompleteHandler_wrapper+0xc5
06 fffff803`5426e6d0 fffff803`53223070 ndis!ndisCallSendCompleteHandler+0x3d07b
07 fffff803`5426e710 fffff80d`47852f45 ndis!NdisMSendNetBufferListsComplete+0x160
08 fffff803`5426e800 fffff80d`478180ca wdiwifi!CPort::SendCompleteNetBufferLists+0x111
09 fffff803`5426e860 fffff80d`47809f71 wdiwifi!CAdapter::SendCompleteNbl+0x12a
0a fffff803`5426e8d0 fffff80d`47809b73 wdiwifi!CTxMgr::CompleteNdisNbl+0xdd
0b fffff803`5426e930 fffff80d`47806746 wdiwifi!CTxMgr::CompleteNBLs+0x5b
0c fffff803`5426e970 fffff80d`477f7f70 wdiwifi!CTxMgr::TxTransferCompleteInd+0x68a
0d fffff803`5426ea30 fffff80d`4725b1ba wdiwifi!AdapterTxTransferCompleteInd+0x10
0e fffff803`5426ea60 fffff80d`472df42e Netwtw10+0xb1ba
0f fffff803`5426eb50 fffff80d`47581a65 Netwtw10+0x8f42e
10 fffff803`5426ec80 fffff80d`475840b1 Netwtw10+0x331a65
11 fffff803`5426ecc0 fffff80d`475a1976 Netwtw10+0x3340b1
12 fffff803`5426ed50 fffff80d`4757691d Netwtw10+0x351976
0: kd> .frame /r 3
03 fffff803`5426e610 fffff803`5406e6ed nwifi!Dot11SendCompletion+0x35
rax=0000000000000000 rbx=ffffdf8f000ffff8 rcx=ffff888b054f2d90
rdx=ffff888b05519da0 rsi=ffff888b05519da0 rdi=ffff888b054f2dd0
rip=fffff8035406a5b5 rsp=fffff8035426e610 rbp=0000000000000000
 r8=0000000000000000  r9=fffff80353303048 r10=0000000000000000
r11=0000000000000018 r12=fffff8035406e6d0 r13=ffff888afa3c2810
r14=0000000000000000 r15=ffff888afa3c2810
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+0x35:
fffff803`5406a5b5 488b03          mov     rax,qword ptr [rbx] ds:002b:ffffdf8f`000ffff8=????????????????
0: kd> !ndiskd.nbl -log ffff888b05519da0

    Allocated
    FilterSent          ffff888afb58ca20 - Virtual WiFi Filter Driver-0000
    FilterSent          ffff888afb498a20 - WFP Native MAC Layer LightWeight Filter-0000
    FilterSent          ffff888aflcdf1a0 - Intel(R) Wi-Fi 6 AX201 160MHz
    SentToMiniport      ffff888aflcdf1a0 - Intel(R) Wi-Fi 6 AX201 160MHz
    MiniportSendCompleted ffff888afb498a20 - WFP Native MAC Layer LightWeight Filter-0000
    FilterSendCompleted ffff888afb58ca20 - Virtual WiFi Filter Driver-0000
    FilterSendCompleted ffff888afb591a20 - NDIS Sample LightWeight Filter 1-0000
    FilterSendCompleted ffff888afb590a20 - Native WiFi Filter Driver-0000
```

```
0: kd> !nbl ffff888b05519da0
    NBL                 ffff888b05519da0    Next NBL            NULL
    First NB            ffff888b05519f20    Source              ffff888afb591a20 - NDIS Sample LightWeight Filter 1-0000
    Context stack       ffff888b054f2d90    Pool                ffff888afb58d040 -
    Flags               NBL ALLOCATED, NBL CONTEXT ALLOCATED

    Walk the NBL chain                      Dump data payload
    Show out-of-band information            Show in Microsoft Network Monitor
    Review NBL history

0: kd> !ndiskd.nblpool ffff888afb58d040


NBL POOL

    Ndis handle         ffff888afb58d040
    Allocation tag      Filt
    Owner
    Allocated by        vwifimf+1822

    Flags               CONTAINS NET BUFFER
    Structure size      0n560
    Context size        0
    Data size           0
0: kd> !ndiskd.filterdriver ffff888af121ac30


FILTER DRIVER

    NDIS Sample LightWeight Filter 1

    Ndis handle         ffff888af121ac30
    Driver context      ffff888af121aa70
    Ndis API version    v6.0
    Driver version      v1.0
    Driver object       ffff888af121aa70
    Driver image        vwifimf.sys

    Bind flags          Mandatory, Modifying, UnbindOnAttach, UnbindOnDetach
    Class               Cannot find field '_p' in 'class wistd::unique_ptr >'
    References          2
```

以下为 vwifimf 的版本信息，请检查是否为当前案例处理的 TMS 版本

```
0: kd> lmvm vwifimf
Browse full module list
start             end                 module name
fffff80d`44af0000 fffff80d`44afb000   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:        Mon Dec 14 14:35:49 2020 (5FD707C5)
    CheckSum:         0000C71F
    ImageSize:        0000B000
    Translations:     0000.04b0 0000.04e4 0409.04b0 0409.04e4
    Information from resource tables:
```

下一步动作:

建议与 case：CAS-05796-S4W5H4 一并处理。

李琦 Li Qi
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话： 4008180055
电子邮箱 Email: liqi@cmgos.com

发件人: Li Qi
发送时间: 2022 年 4 月 25 日 15:43
收件人: 许翔 <windowsserversupport@sdc.icbc.com.cn>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>; 'win10 升级支持' <win10sup@sdc.icbc.com.cn>
主题: 回复: [案例号: CAS-06133-X9Z4Q7] % |P2|ICBC|软件开发中心政府版系统异常蓝屏问题 % 初次响应 CMIT:0001362

许先生，您好:

如刚才电话沟通，谨以此封邮件阐述我们双方针对这个问题所涉及范围界定:

问题定义:

用户反馈软件开发中心出现 2 台电脑出现偶发性蓝屏，已上传相关 dump 日志。

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。

李琦 Li Qi
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话: 4008180055
电子邮箱 Email: liqi@cmgos.com

发件人: Li Qi <liqi@cmgos.com>
发送时间: 2022 年 4 月 25 日 15:27
收件人: 许翔 <windowsserversupport@sdc.icbc.com.cn>
抄送: Li Qi <liqi@cmgos.com>
主题: [案例号: CAS-06133-X9Z4Q7] % |P2|ICBC|软件开发中心政府版系统异常蓝屏问题 % 初次响应 CMIT:0001362

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 李琦 。 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-06133-X9Z4Q7 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”。