吴先生，您好!

很高兴与您电话沟通，根据沟通的结果，我将暂时归档此问题。**案例归档后您会收到调查问卷的邮件，希望可以对我们的服务进行评价。**
工单的归档并不会影响我们为您提供技术支持服务，如果您的问题复现，或有新的问题出现，您也可以致电我们的技术支持热线 4008180055。

案例总结：
案例描述：
用户在连接 ICBCOTP 时发生蓝屏。

案例进展：
已经使用不勾选启用对主密钥 PMK 缓存的方式、以及更新网卡驱动的临时解决方案解决，归档案例。

案例分析：

MEMORY_WUZONG.DMP 这台机器是蓝屏原因是由于 authcomm.sys 导致的。

日志分析：

```
2: kd> !mex.crash
Dump Info
==========================================
Dump Name: MEMORY_WUZONG.DMP
Windows 10 Kernel Version 17763 MP (4 procs) Free x64
Product: WinNt, suite: TerminalServer SingleUserTS
Edition build lab: 17763.1.amd64fre.rs5_release.180914-1434
Kernel base = 0xfffff801`7940a000 PsLoadedModuleList = 0xfffff801`798213d0
Debug session time: Sat Jun 19 18:42:43.041 2021 (UTC + 8:00)
System Uptime: 3 days 9:26:22.085
SystemManufacturer = LENOVO
SystemProductName = 20JTS2LF00
Processor: Intel(R) Core(TM) i5-6200U CPU @ 2.30GHz
Bugcheck: D1 (0, 2, 8, 0)
Kernel Complete Dump File: Full address space is available.


Bugcheck details
==========================================
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

Crashing Stack
================================================
Process                 Thread          CID      UserTime KernelTime ContextSwitches Wait Reason
Time State
scauth.exe *32 (ffff8684f588f080) ffff8684f77aa080 10f8.18f8    203ms     469ms          6608
Executive     0s Running on CPU 2  >>崩溃线程、进程信息

Irp List:
   IRP           File Driver
   ffff8685002f9e20      Authcomm >> 可疑的驱动

# Child-SP        Return          Call Site
0 fffff3007e917218 fffff801795d2de9 nt!KeBugCheckEx+0x0
1 fffff3007e917220 fffff801795cf1d4 nt!KiBugCheckDispatch+0x69
2 fffff3007e917360 0000000000000000 nt!KiPageFault+0x454

This thread is crashing

2: kd> .trap fffff3007e917360
NOTE: The trap frame does not contain all registers.
Some register values may be zeroed or incorrect.
rax=0000000000000000 rbx=0000000000000000 rcx=ffff8684ff066bd0
rdx=ffff8684fb1f9ea0 rsi=0000000000000000 rdi=0000000000000000
rip=0000000000000000 rsp=fffff3007e9174f8 rbp=0000000000000600
r8=ffff8684fb1f9ea0  r9=ffff8684ff066bd0 r10=0000000000000002
r11=fffff3007e917500 r12=0000000000000000 r13=0000000000000000
r14=0000000000000000 r15=0000000000000000
iopl=0         nv up ei ng nz na po nc
00000000`00000000 ??              ???

2: kd> k
# Child-SP        RetAddr           Call Site
00 fffff300`7e9174f8 fffff801`7cc7f0ef     0x0
01 fffff300`7e917500 fffff801`7d402a95     ndis!NdisRequest+0x1f //这里访问了 0 地址。
02 fffff300`7e917530 fffff801`7d4019f8     authcomm+0x2a95 >>怀疑为 authcomm 造成蓝屏
03 fffff300`7e917560 fffff801`7d4021f6     authcomm+0x19f8
04 fffff300`7e917590 fffff801`7d401369     authcomm+0x21f6
05 fffff300`7e917630 fffff801`7d4020d9     authcomm+0x1369
06 fffff300`7e9176a0 fffff801`79483f39     authcomm+0x20d9
07 (Inline Function) --------`--------     nt!IopfCallDriver+0x44
08 fffff300`7e9176f0 fffff801`79a23811     nt!IofCallDriver+0x59
09 (Inline Function) --------`--------     nt!IoCallDriverWithTracing+0x2b
0a (Inline Function) --------`--------     nt!IopCallDriverReference+0xbd
```

```
0b fffff300`7e917730 fffff801`79a2357c     nt!IopSynchronousServiceTail+0x1b1
0c fffff300`7e9177e0 fffff801`79a23646     nt!IopXxxControlFile+0xe0c
0d fffff300`7e917920 fffff801`795d2805     nt!NtDeviceIoControlFile+0x56
0e fffff300`7e917990 00000000`77881cbc     nt!KiSystemServiceCopyEnd+0x25
0f 00000000`019aeb88 00000000`778818f3     wow64cpu!CpupSyscallStub+0xc
10 00000000`019aeb90 00000000`77881199     wow64cpu!DeviceIoctlFileFault+0x31
11 00000000`019aec40 00007ffc`b15acfda     wow64cpu!BTCpuSimulate+0x9
12 (Inline Function) --------`--------     wow64!CpuSimulate+0x6
13 00000000`019aec80 00007ffc`b15acea0     wow64!RunCpuSimulation+0xa
14 00000000`019aecb0 00007ffc`b22d863d     wow64!Wow64LdrpInitialize+0x120
15 (Inline Function) --------`--------     ntdll!Wow64LdrpInitialize+0x9
16 00000000`019aef60 00007ffc`b22d8223     ntdll!_LdrpInitialize+0x401
17 00000000`019af000 00007ffc`b22d81ce     ntdll!LdrpInitialize+0x3b
18 00000000`019af030 00000000`00000000     ntdll!LdrInitializeThunk+0xe
```

细节分析：

```
2: kd> .frame 0n1;dv /t /v
01 fffff300`7e917500 fffff801`7d402a95     ndis!NdisRequest+0x1f
@rbx            int * Status = 0x00000000`00000000
<unavailable>     void * NdisBindingHandle = <value unavailable>  >>参数不正确
<unavailable>     struct _NDIS_REQUEST * NdisRequest = <value unavailable>

2: kd> r
Last set context:
rax=0000000000000000 rbx=0000000000000000 rcx=ffff8684ff066bd0
rdx=ffff8684fb1f9ea0 rsi=0000000000000000 rdi=0000000000000000
rip=0000000000000000 rsp=fffff3007e9174f8 rbp=0000000000000600
r8=ffff8684fb1f9ea0  r9=ffff8684ff066bd0 r10=0000000000000002
r11=fffff3007e917500 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
00000000`00000000 ??              ???

2: kd> ub fffff801`7d402a95
authcomm+0x2a75:
fffff801`7d402a75 894320        mov     dword ptr [rbx+20h],eax
fffff801`7d402a78 488d573c      lea     rdx,[rdi+3Ch]
fffff801`7d402a7c 488d4c2438    lea     rcx,[rsp+38h]
fffff801`7d402a81 48895330      mov     qword ptr [rbx+30h],rdx
fffff801`7d402a85 488b17        mov     rdx,qword ptr [rdi]
fffff801`7d402a88 4c8bc3        mov     r8,rbx
fffff801`7d402a8b 89442438      mov     dword ptr [rsp+38h],eax
fffff801`7d402a8f ff15d3150000  call    qword ptr [authcomm+0x4068 (fffff801`7d404068)]

2: kd> dq ffff8684fb1f9ea0
ffff8684`fb1f9ea0  00000000`00000000 00000000`00000000
ffff8684`fb1f9eb0  00000000`00000000 00000000`00000000
```

```
ffff8684`fb1f9ec0  00000000`00000000 00000000`01010102
ffff8684`fb1f9ed0  ffff8684`ecbb0cdc 00000004`00000006
ffff8684`fb1f9ee0  00000000`00000000 00000000`00000000
ffff8684`fb1f9ef0  00000000`00000000 00000000`00000000
ffff8684`fb1f9f00  00000000`00000000 00000000`00000000
ffff8684`fb1f9f10  00000000`00000000 00000000`00000000
```

//经过 code review，问题的直接原因是 NdisBindingHandle 这个参数不对，而这个参数是在处理 authcomm 相关行为的时候通过 R8 传过来的。所以，问题出在 authcomm。

```
2: kd> lmvm authcomm
Browse full module list
start             end                 module name
fffff801`7d400000 fffff801`7d408000   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 Mar 24 09:06:45 2021 (605A90A5)
    CheckSum:         0000C0B8
    ImageSize:        00008000
    Translations:     0000.04b0 0000.04e4 0409.04b0 0409.04e4
    Information from resource tables:
```

MEMORY_pengwh.DMP 这个机器的问题出在 vwifimf.sys，与之前所处理过的问题一样。

```
0: kd> !mex.crash
Dump Info
==========================================
Dump Name: MEMORY_pengwh.DMP
Windows 10 Kernel Version 17763 MP (8 procs) Free x64
Product: WinNt, suite: TerminalServer SingleUserTS
Edition build lab: 17763.1.amd64fre.rs5_release.180914-1434
Kernel base = 0xfffff805`6aa13000 PsLoadedModuleList = 0xfffff805`6ae2e670
Debug session time: Fri Jun 25 10:45:35.239 2021 (UTC + 8:00)
System Uptime: 0 days 0:04:46.378
SystemManufacturer = LENOVO
SystemProductName = 20NYS4MA00
Processor: Intel(R) Core(TM) i7-8565U CPU @ 1.80GHz
Bugcheck: D1 (FFFFFE82000FFFF8, 2, 0, FFFFF80573A094FD)
Kernel Summary Dump File: Kernel address space is available, User address space may not be
available.


Bugcheck details
==========================================
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: fffffe82000ffff8, memory referenced
Arg2: 0000000000000002, IRQL
Arg3: 0000000000000000, value 0 = read operation, 1 = write operation
Arg4: fffff80573a094fd, address which referenced memory

Crashing Stack
================================================
Process             AttachedProcess         Thread          CID      UserTime KernelTime
ContextSwitches Wait Reason Time State
Idle (fffff8056af709c0) System (ffffdd02c9ca8040) fffff8056af73400
0.0           0s  2m:33.156         167935 Executive     0s Running on CPU 0

# Child-SP        Return          Call Site
 0 fffff8056d478af8 fffff8056abd88e9 nt!KeBugCheckEx+0x0
 1 fffff8056d478b00 fffff8056abd4cd4 nt!KiBugCheckDispatch+0x69
 2 fffff8056d478c40 fffff80573a094fd nt!KiPageFault+0x454
 3 fffff8056d478dd0 fffff80573a0d66d nwifi!Dot11SendCompletion+0x35
 4 fffff8056d478e10 fffff80570e366a3 nwifi!Pt6SendComplete+0x1d
 5 fffff8056d478e40 fffff80570e31efd ndis!ndisCallSendCompleteHandler+0x33
 6 (Inline)        ---------------- ndis!ndisIterativeDPInvokeHandlerOnTracker+0x44
 7 (Inline)        ---------------- ndis!ndisInvokeNextSendCompleteHandler+0xcb
 8 (Inline)        ---------------- ndis!ndisMSendNetBufferListsCompleteInternal+0x211
 9 fffff8056d478e80 fffff8057670593d ndis!NdisMSendNetBufferListsComplete+0x26d
 a fffff8056d478f90 fffff805766d2ef0 wdiwifi!CPort::SendCompleteNetBufferLists+0xf5
 b fffff8056d478fe0 fffff805766c74da wdiwifi!CAdapter::SendCompleteNbl+0x11c
 c fffff8056d479050 fffff805766c71f1 wdiwifi!CTxMgr::CompleteNdisNbl+0xbe
 d fffff8056d4790b0 fffff805766c4395 wdiwifi!CTxMgr::CompleteNBLs+0x59
 e fffff8056d4790f0 fffff805766b7440 wdiwifi!CTxMgr::TxTransferCompleteInd+0x5c9
 f fffff8056d4791b0 fffff80575dd9cf8 wdiwifi!AdapterTxTransferCompleteInd+0x10
10 fffff8056d4791e0 fffff80575e2d0f6 Netwtw08+0x49cf8
11 fffff8056d479240 fffff805761c9850 Netwtw08+0x9d0f6
12 fffff8056d479370 fffff805761d6882 Netwtw08+0x439850
13 fffff8056d4793a0 fffff805761fb16e Netwtw08+0x446882
14 fffff8056d479400 fffff805761cdbb2 Netwtw08+0x46b16e
15 fffff8056d479500 fffff805761c5dc3 Netwtw08+0x43dbb2
16 fffff8056d4795f0 fffff805761c4881 Netwtw08+0x435dc3
17 fffff8056d479650 fffff805761c590b Netwtw08+0x434881
18 fffff8056d4796b0 fffff80570e36838 Netwtw08+0x43590b
19 (Inline)        ---------------- ndis!ndisMiniportDpc+0xe6
1a fffff8056d4796e0 fffff8056aa8c727 ndis!ndisInterruptDpc+0x188
1b fffff8056d479810 fffff8056aa8bd6e nt!KiExecuteAllDpcs+0x2e7
1c fffff8056d479950 fffff8056abcaa7a nt!KiRetireDpcList+0x1ae
1d fffff8056d479b60 0000000000000000 nt!KiIdleLoop+0x5a

This thread is crashing
```

```
0: kd> .frame /r 0x3; !mex.x
03 fffff805`6d478dd0 fffff805`73a0d66d     nwifi!Dot11SendCompletion+0x35
rax=0000000000000000 rbx=fffffe82000ffff8 rcx=ffffdd02d8bf9e00
rdx=ffffdd02d7bb2da0 rsi=ffffdd02d7bb2da0 rdi=ffffdd02d8bf9e40
rip=fffff80573a094fd rsp=fffff8056d478dd0 rbp=0000000000000000
r8=0000000000000000  r9=0000000000000000 r10=0000000000000001
r11=ffffdd02d46cb290 r12=ffffdd02d415c760 r13=ffffdd02d4181020
r14=ffffdd02d2d19c18 r15=ffffdd02d415cb00
iopl=0         nv up ei ng nz na po nc
cs=0010  ss=0018  ds=002b  es=002b  fs=0053  gs=002b             efl=00000286
nwifi!Dot11SendCompletion+0x35:
fffff805`73a094fd 488b03          mov     rax,qword ptr [rbx]
ds:002b:fffffe82`000ffff8=????????????????
@rsi            pNdisPacket = 0xffffdd02`d7bb2da0 _NET_BUFFER_LIST
@ebp             ndisStatus = 0n0
@rdi            pBOS = 0xffffdd02`d8bf9e40
@rbx             pTOS = 0xfffffe82`000ffff8

0: kd> dt 0xffffdd02`d7bb2da0 nwifi!_NET_BUFFER_LIST
_NET_BUFFER_LIST
   +0x000 Next           : (null)
   +0x008 FirstNetBuffer   : 0xffffdd02`d7bb2f20  _NET_BUFFER
   +0x000 Link           : _SLIST_HEADER
   +0x000 NetBufferListHeader : _NET_BUFFER_LIST_HEADER
   +0x010 Context        : 0xffffdd02`d8bf9e00 _NET_BUFFER_LIST_CONTEXT
   +0x018 ParentNetBufferList : (null)
   +0x020 NdisPoolHandle   : 0xffffdd02`d1474080 Void
   +0x030 NdisReserved     : [2] (null)
   +0x040 ProtocolReserved : [4] 0xffffdd02`d9af69c0 Void
   +0x060 MiniportReserved : [2] (null)
   +0x070 Scratch        : (null)
   +0x078 SourceHandle     : 0xffffdd02`d2d19850 Void
   +0x080 NblFlags       : 0
   +0x084 ChildRefCount    : 0n0
   +0x088 Flags          : 0x500
   +0x08c Status         : 0n0
   +0x08c NdisReserved2    : 0
   +0x090 NetBufferListInfo : [26] (null)

0: kd> !pool 0xffffdd02`d1474080
Pool page ffffdd02d1474080 region is Nonpaged pool
ffffdd02d1474000 size:   30 previous size:    0  (Free)       ....
*ffffdd02d1474040 size:  a00 previous size:    0  (Allocated) *Filt  >>问题出在此 Tag
                        Owning component : Unknown (update pooltag.txt)
ffffdd02d1474a50 size:  3f0 previous size:    0  (Allocated)  TcpE
ffffdd02d1474e40 size:  1a0 previous size:    0  (Free)       ..eB

0: kd> !mex.tag Filt
```

```
Unable to load image \SystemRoot\system32\DRIVERS\vwifimf.sys, Win32 error 0n2
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
============================================
fffff805`71f81790  41 b8 46 69 6c 74 03 d1-0f b7 08 8d 94 0a 08 01  A.Filt.........
```

贾伟 Jia Wei
神州网信技术有限公司
服务支持电话： 400-818-0055
电子邮箱： jiawei@cmgos.com

C&M Information Technologies Co., Ltd.
11F, Block C North Building, Raycom InfoTech Park, Beijing
mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人: Jia Wei
发送时间: 2021 年 7 月 5 日 16:10
收件人: 'win10 升级支持' <win10sup@sdc.icbc.com.cn>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>; Liu Jian <liujian@cmgos.com>; '李粤' <liyue@sdc.icbc.com.cn>
主题: 回复: 【外来邮件，注意核实】回复: [案例号: CAS-04372-M5F9L9] % |P3|ICBC|V0-H 升级 V2020-L 使用无线蓝屏 % 初次响应 CMIT:0001150

吴先生 您好，

来信是想咨询当前案件进展状况。

如果针对当前案件还有需要我们帮助的地方，欢迎随时联系我们。

贾伟 Jia Wei
神州网信技术有限公司

服务支持电话： 400-818-0055
电子邮箱： jiawei@cmgos.com

C&M Information Technologies Co., Ltd.
11F, Block C North Building, Raycom InfoTech Park, Beijing
mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人: Jia Wei
发送时间: 2021 年 7 月 1 日 9:58
收件人: 'win10 升级支持' <win10sup@sdc.icbc.com.cn>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>; Liu Jian <liujian@cmgos.com>; '李粤' <liyue@sdc.icbc.com.cn>
主题: 回复: 【外来邮件，注意核实】回复: [案例号: CAS-04372-M5F9L9] % |P3|ICBC|V0-H 升级 V2020-L 使用无线蓝屏 % 初次响应 CMIT:0001150

吴先生您好，

MEMORY_WUZONG.DMP 这台机器是蓝屏原因是由于 authcomm.sys 导致的。

日志分析：

```
2: kd> !mex.crash
Dump Info
==========================================
Dump Name: MEMORY_WUZONG.DMP
Windows 10 Kernel Version 17763 MP (4 procs) Free x64
Product: WinNt, suite: TerminalServer SingleUserTS
Edition build lab: 17763.1.amd64fre.rs5_release.180914-1434
Kernel base = 0xfffff801`7940a000 PsLoadedModuleList = 0xfffff801`798213d0
Debug session time: Sat Jun 19 18:42:43.041 2021 (UTC + 8:00)
System Uptime: 3 days 9:26:22.085
SystemManufacturer = LENOVO
SystemProductName = 20JTS2LF00
Processor: Intel(R) Core(TM) i5-6200U CPU @ 2.30GHz
Bugcheck: D1 (0, 2, 8, 0)
Kernel Complete Dump File: Full address space is available.


Bugcheck details
==========================================
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

Crashing Stack
================================================
Process                Thread         CID      UserTime KernelTime ContextSwitches Wait Reason
Time State
scauth.exe *32 (ffff8684f588f080) ffff8684f77aa080 10f8.18f8    203ms     469ms          6608
Executive    0s Running on CPU 2  >>崩溃线程、进程信息

Irp List:
   IRP           File Driver
   ffff8685002f9e20      Authcomm >> 可疑的驱动

# Child-SP        Return         Call Site
0 fffff3007e917218 fffff801795d2de9 nt!KeBugCheckEx+0x0
1 fffff3007e917220 fffff801795cf1d4 nt!KiBugCheckDispatch+0x69
2 fffff3007e917360 0000000000000000 nt!KiPageFault+0x454

This thread is crashing

2: kd> .trap fffff3007e917360
NOTE: The trap frame does not contain all registers.
Some register values may be zeroed or incorrect.
rax=0000000000000000 rbx=0000000000000000 rcx=ffff8684ff066bd0
rdx=ffff8684fb1f9ea0 rsi=0000000000000000 rdi=0000000000000000
rip=0000000000000000 rsp=fffff3007e9174f8 rbp=0000000000000600
r8=ffff8684fb1f9ea0  r9=ffff8684ff066bd0 r10=0000000000000002
r11=fffff3007e917500 r12=0000000000000000 r13=0000000000000000
r14=0000000000000000 r15=0000000000000000
iopl=0         nv up ei ng nz na po nc
00000000`00000000 ??              ???

2: kd> k
# Child-SP        RetAddr           Call Site
00 fffff300`7e9174f8 fffff801`7cc7f0ef     0x0
01 fffff300`7e917500 fffff801`7d402a95     ndis!NdisRequest+0x1f //这里访问了 0 地址。
02 fffff300`7e917530 fffff801`7d4019f8     authcomm+0x2a95 >>怀疑为 authcomm 造成蓝屏
03 fffff300`7e917560 fffff801`7d4021f6     authcomm+0x19f8
04 fffff300`7e917590 fffff801`7d401369     authcomm+0x21f6
05 fffff300`7e917630 fffff801`7d4020d9     authcomm+0x1369
06 fffff300`7e9176a0 fffff801`79483f39     authcomm+0x20d9
07 (Inline Function) --------`--------     nt!IopfCallDriver+0x44
08 fffff300`7e9176f0 fffff801`79a23811     nt!IofCallDriver+0x59
09 (Inline Function) --------`--------     nt!IoCallDriverWithTracing+0x2b
```

```
0a (Inline Function) --------`--------     nt!IopCallDriverReference+0xbd
0b fffff300`7e917730 fffff801`79a2357c     nt!IopSynchronousServiceTail+0x1b1
0c fffff300`7e9177e0 fffff801`79a23646     nt!IopXxxControlFile+0xe0c
0d fffff300`7e917920 fffff801`795d2805     nt!NtDeviceIoControlFile+0x56
0e fffff300`7e917990 00000000`77881cbc     nt!KiSystemServiceCopyEnd+0x25
0f 00000000`019aeb88 00000000`778818f3     wow64cpu!CpupSyscallStub+0xc
10 00000000`019aeb90 00000000`77881199     wow64cpu!DeviceIoctlFileFault+0x31
11 00000000`019aec40 00007ffc`b15acfda     wow64cpu!BTCpuSimulate+0x9
12 (Inline Function) --------`--------     wow64!CpuSimulate+0x6
13 00000000`019aec80 00007ffc`b15acea0     wow64!RunCpuSimulation+0xa
14 00000000`019aecb0 00007ffc`b22d863d     wow64!Wow64LdrpInitialize+0x120
15 (Inline Function) --------`--------     ntdll!Wow64LdrpInitialize+0x9
16 00000000`019aef60 00007ffc`b22d8223     ntdll!_LdrpInitialize+0x401
17 00000000`019af000 00007ffc`b22d81ce     ntdll!LdrpInitialize+0x3b
18 00000000`019af030 00000000`00000000     ntdll!LdrInitializeThunk+0xe
```

细节分析：

```
2: kd> .frame 0n1;dv /t /v
01 fffff300`7e917500 fffff801`7d402a95     ndis!NdisRequest+0x1f
@rbx           int * Status = 0x00000000`00000000
<unavailable>     void * NdisBindingHandle = <value unavailable>  >>参数不正确
<unavailable>     struct _NDIS_REQUEST * NdisRequest = <value unavailable>

2: kd> r
Last set context:
rax=0000000000000000 rbx=0000000000000000 rcx=ffff8684ff066bd0
rdx=ffff8684fb1f9ea0 rsi=0000000000000000 rdi=0000000000000000
rip=0000000000000000 rsp=fffff3007e9174f8 rbp=0000000000000600
r8=ffff8684fb1f9ea0  r9=ffff8684ff066bd0 r10=0000000000000002
r11=fffff3007e917500 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
00000000`00000000 ??              ???

2: kd> ub fffff801`7d402a95
authcomm+0x2a75:
fffff801`7d402a75 894320        mov     dword ptr [rbx+20h],eax
fffff801`7d402a78 488d573c      lea     rdx,[rdi+3Ch]
fffff801`7d402a7c 488d4c2438    lea     rcx,[rsp+38h]
fffff801`7d402a81 48895330      mov     qword ptr [rbx+30h],rdx
fffff801`7d402a85 488b17        mov     rdx,qword ptr [rdi]
fffff801`7d402a88 4c8bc3        mov     r8,rbx
fffff801`7d402a8b 89442438      mov     dword ptr [rsp+38h],eax
fffff801`7d402a8f ff15d3150000  call    qword ptr [authcomm+0x4068 (fffff801`7d404068)]

2: kd> dq ffff8684fb1f9ea0
ffff8684`fb1f9ea0  00000000`00000000 00000000`00000000
```

```
ffff8684`fb1f9eb0  00000000`00000000 00000000`00000000
ffff8684`fb1f9ec0  00000000`00000000 00000000`01010102
ffff8684`fb1f9ed0  ffff8684`ecbb0cdc 00000004`00000006
ffff8684`fb1f9ee0  00000000`00000000 00000000`00000000
ffff8684`fb1f9ef0  00000000`00000000 00000000`00000000
ffff8684`fb1f9f00  00000000`00000000 00000000`00000000
ffff8684`fb1f9f10  00000000`00000000 00000000`00000000
```

//经过 code review，问题的直接原因是 NdisBindingHandle 这个参数不对，而这个参数是在处理 authcomm 相关行为的时候通过 R8 传过来的。所以，问题出在 authcomm。

```
2: kd> lmvm authcomm
Browse full module list
start             end                 module name
fffff801`7d400000 fffff801`7d408000   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 Mar 24 09:06:45 2021 (605A90A5)
    CheckSum:         0000C0B8
    ImageSize:        00008000
    Translations:     0000.04b0 0000.04e4 0409.04b0 0409.04e4
    Information from resource tables:
```

MEMORY_pengwh.DMP 这个机器的问题出在 vwifimf.sys，与之前所处理过的问题一样。

```
0: kd> !mex.crash
Dump Info
==========================================
Dump Name: MEMORY_pengwh.DMP
Windows 10 Kernel Version 17763 MP (8 procs) Free x64
Product: WinNt, suite: TerminalServer SingleUserTS
Edition build lab: 17763.1.amd64fre.rs5_release.180914-1434
Kernel base = 0xfffff805`6aa13000 PsLoadedModuleList = 0xfffff805`6ae2e670
Debug session time: Fri Jun 25 10:45:35.239 2021 (UTC + 8:00)
System Uptime: 0 days 0:04:46.378
SystemManufacturer = LENOVO
SystemProductName = 20NYS4MA00
Processor: Intel(R) Core(TM) i7-8565U CPU @ 1.80GHz
Bugcheck: D1 (FFFFFE82000FFFF8, 2, 0, FFFFF80573A094FD)
Kernel Summary Dump File: Kernel address space is available, User address space may not be
available.


Bugcheck details
==========================================
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: fffffe82000ffff8, memory referenced
Arg2: 0000000000000002, IRQL
Arg3: 0000000000000000, value 0 = read operation, 1 = write operation
Arg4: fffff80573a094fd, address which referenced memory

Crashing Stack
=========================================
Process             AttachedProcess         Thread          CID      UserTime KernelTime
ContextSwitches Wait Reason Time State
Idle (fffff8056af709c0) System (ffffdd02c9ca8040) fffff8056af73400
0.0           0s  2m:33.156         167935 Executive     0s Running on CPU 0

# Child-SP        Return          Call Site
 0 fffff8056d478af8 fffff8056abd88e9 nt!KeBugCheckEx+0x0
 1 fffff8056d478b00 fffff8056abd4cd4 nt!KiBugCheckDispatch+0x69
 2 fffff8056d478c40 fffff80573a094fd nt!KiPageFault+0x454
 3 fffff8056d478dd0 fffff80573a0d66d nwifi!Dot11SendCompletion+0x35
 4 fffff8056d478e10 fffff80570e366a3 nwifi!Pt6SendComplete+0x1d
 5 fffff8056d478e40 fffff80570e31efd ndis!ndisCallSendCompleteHandler+0x33
 6 (Inline)        ---------------- ndis!ndisIterativeDPInvokeHandlerOnTracker+0x44
 7 (Inline)        ---------------- ndis!ndisInvokeNextSendCompleteHandler+0xcb
 8 (Inline)        ---------------- ndis!ndisMSendNetBufferListsCompleteInternal+0x211
 9 fffff8056d478e80 fffff8057670593d ndis!NdisMSendNetBufferListsComplete+0x26d
 a fffff8056d478f90 fffff805766d2ef0 wdiwifi!CPort::SendCompleteNetBufferLists+0xf5
 b fffff8056d478fe0 fffff805766c74da wdiwifi!CAdapter::SendCompleteNbl+0x11c
 c fffff8056d479050 fffff805766c71f1 wdiwifi!CTxMgr::CompleteNdisNbl+0xbe
 d fffff8056d4790b0 fffff805766c4395 wdiwifi!CTxMgr::CompleteNBLs+0x59
 e fffff8056d4790f0 fffff805766b7440 wdiwifi!CTxMgr::TxTransferCompleteInd+0x5c9
 f fffff8056d4791b0 fffff80575dd9cf8 wdiwifi!AdapterTxTransferCompleteInd+0x10
10 fffff8056d4791e0 fffff80575e2d0f6 Netwtw08+0x49cf8
11 fffff8056d479240 fffff805761c9850 Netwtw08+0x9d0f6
12 fffff8056d479370 fffff805761d6882 Netwtw08+0x439850
13 fffff8056d4793a0 fffff805761fb16e Netwtw08+0x446882
14 fffff8056d479400 fffff805761cdbb2 Netwtw08+0x46b16e
15 fffff8056d479500 fffff805761c5dc3 Netwtw08+0x43dbb2
16 fffff8056d4795f0 fffff805761c4881 Netwtw08+0x435dc3
17 fffff8056d479650 fffff805761c590b Netwtw08+0x434881
18 fffff8056d4796b0 fffff80570e36838 Netwtw08+0x43590b
19 (Inline)        ---------------- ndis!ndisMiniportDpc+0xe6
1a fffff8056d4796e0 fffff8056aa8c727 ndis!ndisInterruptDpc+0x188
1b fffff8056d479810 fffff8056aa8bd6e nt!KiExecuteAllDpcs+0x2e7
1c fffff8056d479950 fffff8056abcaa7a nt!KiRetireDpcList+0x1ae
1d fffff8056d479b60 0000000000000000 nt!KiIdleLoop+0x5a

This thread is crashing
```

```
0: kd> .frame /r 0x3; !mex.x
03 fffff805`6d478dd0 fffff805`73a0d66d     nwifi!Dot11SendCompletion+0x35
rax=0000000000000000 rbx=fffffe82000ffff8 rcx=ffffdd02d8bf9e00
rdx=ffffdd02d7bb2da0 rsi=ffffdd02d7bb2da0 rdi=ffffdd02d8bf9e40
rip=fffff80573a094fd rsp=fffff8056d478dd0 rbp=0000000000000000
r8=0000000000000000  r9=0000000000000000 r10=0000000000000001
r11=ffffdd02d46cb290 r12=ffffdd02d415c760 r13=ffffdd02d4181020
r14=ffffdd02d2d19c18 r15=ffffdd02d415cb00
iopl=0         nv up ei ng nz na po nc
cs=0010  ss=0018  ds=002b  es=002b  fs=0053  gs=002b             efl=00000286
nwifi!Dot11SendCompletion+0x35:
fffff805`73a094fd 488b03          mov     rax,qword ptr [rbx]
ds:002b:fffffe82`000ffff8=????????????????
@rsi            pNdisPacket = 0xffffdd02`d7bb2da0 _NET_BUFFER_LIST
@ebp             ndisStatus = 0n0
@rdi            pBOS = 0xffffdd02`d8bf9e40
@rbx             pTOS = 0xfffffe82`000ffff8

0: kd> dt 0xffffdd02`d7bb2da0 nwifi!_NET_BUFFER_LIST
_NET_BUFFER_LIST
   +0x000 Next           : (null)
   +0x008 FirstNetBuffer   : 0xffffdd02`d7bb2f20  _NET_BUFFER
   +0x000 Link           : _SLIST_HEADER
   +0x000 NetBufferListHeader : _NET_BUFFER_LIST_HEADER
   +0x010 Context        : 0xffffdd02`d8bf9e00 _NET_BUFFER_LIST_CONTEXT
   +0x018 ParentNetBufferList : (null)
   +0x020 NdisPoolHandle   : 0xffffdd02`d1474080 Void
   +0x030 NdisReserved     : [2] (null)
   +0x040 ProtocolReserved : [4] 0xffffdd02`d9af69c0 Void
   +0x060 MiniportReserved : [2] (null)
   +0x070 Scratch        : (null)
   +0x078 SourceHandle     : 0xffffdd02`d2d19850 Void
   +0x080 NblFlags       : 0
   +0x084 ChildRefCount    : 0n0
   +0x088 Flags          : 0x500
   +0x08c Status         : 0n0
   +0x08c NdisReserved2    : 0
   +0x090 NetBufferListInfo : [26] (null)

0: kd> !pool 0xffffdd02`d1474080
Pool page ffffdd02d1474080 region is Nonpaged pool
ffffdd02d1474000 size:   30 previous size:    0  (Free)       ....
*ffffdd02d1474040 size:  a00 previous size:    0  (Allocated) *Filt  >>问题出在此 Tag
                        Owning component : Unknown (update pooltag.txt)
ffffdd02d1474a50 size:  3f0 previous size:    0  (Allocated)  TcpE
ffffdd02d1474e40 size:  1a0 previous size:    0  (Free)       ..eB
```

```
0: kd> !mex.tag Filt
Unable to load image \SystemRoot\system32\DRIVERS\vwifimf.sys, Win32 error 0n2
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
============================================
fffff805`71f81790  41 b8 46 69 6c 74 03 d1-0f b7 08 8d 94 0a 08 01  A.Filt.........
```

下一步计划：

查看%SystemRoot%\system32\drivers\authcomm.sys 文件属性，确认是由哪个三方供应商开发。

贾伟 Jia Wei
神州网信技术有限公司
服务支持电话： 400-818-0055
电子邮箱： jiawei@cmgos.com

C&M Information Technologies Co., Ltd.
11F, Block C North Building, Raycom InfoTech Park, Beijing
mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人: Jia Wei
发送时间: 2021 年 6 月 30 日 14:30
收件人: 'win10 升级支持' <win10sup@sdc.icbc.com.cn>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>; Liu Jian <liujian@cmgos.com>; 李粤 <liyue@sdc.icbc.com.cn>
主题: 回复: 【外来邮件，注意核实】回复: [案例号: CAS-04372-M5F9L9] % |P3|ICBC|V0-H 升级 V2020-L 使用无线蓝屏 % 初次响应 CMIT:0001150

吴先生，

很高兴与您电话沟通，当前 2 个 dump 文件其中一个与 vwifimf.sys 有关，另一个还在分析过程中，分析过程邮件我在分析完成之后一并发送给您。
另外如果有其他人员出现蓝屏，您也可以收集 MEMORY.DMP 日志、压缩并上传至 sftp 服务器。

日志上传：

为了更安全、快速地传输数据，您可以在 Filezilla 上使用以下账户信息登入神州网信网站。

- Filezilla client 端下载 URL：https://filezilla-project.org/download.php?type=client
- 登陆地址：sftp://ocean.cmgos.com
- 用户名为：ICBC（区分大小写）
- 密码：2qfs52ninbFB
- 端口：22222

登陆之后，上传至**/upload/蓝屏日志**文件夹

==========

在向 CMIT 提供日志和数据前，请阅读并接受邮件下方隐私声明。

隐私声明

为向您提供本产品的相关技术支持及相关服务，您需要在同意本声明的前提下向神州网信提供为解决系统故障必要的数据和信息，包括但不限于与您相关的个人数据和隐私信息。通常情况下，我们仅需要如下数据以使我们的服务能够更好地满足您的需求：内存转储文件、注册表信息、组策略信息、事件日志、安装应用列表、驱动信息、网络日志或系统补丁等。

神州网信承诺将采取商业上可行及必要措施保护用户提供给神州网信的数据和信息，且仅在解决问题过程中使用。

神州网信保证不对外公开或向第三方提供、公开或共享您提供的数据和信息。

在以下情况下，神州网信对您的数据和信息的披露将不视为违约，具体包括：

(1) 神州网信已获得您的明确授权；

(2) 根据适用法律的要求，神州网信负有披露义务的；
(3) 司法机关或行政机关基于法定程序要求神州网信提供的；
(4) 为维护社会公共利益及神州网信合法权益，在合理范围内进行披露的。
(5) 为了解决您的系统故障问题，神州网信可能会与神州网信的分包商披露您提供的数据和信息。在此情况下，第三方会承担与神州网信同等的隐私保护责任的，神州网信会在合理范围内对您的信息进行披露。
如果您欲提供的数据和信息中包含对您重要的保密信息以及商业秘密，在您向神州网信提供上述数据和信息前，务必对上述数据和信息进行脱敏处理，否则请不要提供该信息给神州网信。作为一家商业软件公司，神州网信在商业可行的前提下，已为用户的数据和信息保护做了极大的努力，但是仍然不能保证现有的安全技术措施使您的数据和信息等不受任何形式的损失。您对上述情况充分知情，且不会因此追究神州网信的法律责任。

贾伟 Jia Wei
神州网信技术有限公司
服务支持电话： 400-818-0055
电子邮箱： jiawei@cmgos.com

C&M Information Technologies Co., Ltd.
11F, Block C North Building, Raycom InfoTech Park, Beijing
mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人: win10 升级支持 <win10sup@sdc.icbc.com.cn>
发送时间: 2021 年 6 月 30 日 14:06
收件人: Jia Wei <jiawei@cmgos.com>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>; Liu Jian <liujian@cmgos.com>; 李粤 <liyue@sdc.icbc.com.cn>
主题: 答复: 【外来邮件，注意核实】回复: [案例号: CAS-04372-M5F9L9] % |P3|ICBC|V0-H 升级 V2020-L 使用无线蓝屏 % 初次响应 CMIT:0001150

贾工
目前 dump 分析的进展如何？本周又有部门领导发生蓝屏，请尽快定位问题原因。

发件人: "Jia Wei" <jiawei@cmgos.com>
收件人: "吴毓杰" <win10sup@sdc.icbc.com.cn>
抄送: "ICBC_Notification" <ICBC_Notification@cmgos.com>
日期: 2021/06/29 10:16

主题: 【外来邮件，注意核实】回复: [案例号: CAS-04372-M5F9L9] % |P3|ICBC|V0-H 升级 V2020-L 使用无线蓝屏 % 初次响应 CMIT:0001150

吴先生，您好

很高兴与您取得电话沟通，我们正在着手分析日志，如果有进展将立即与您取得沟通。

问题定义：
用户在连接 ICBCOTP 时发生蓝屏。目前使用对于无线设置配置的临时解决方案蓝屏暂时不再复现，仍需要找到问题根本原因。

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。

贾伟 Jia Wei
神州网信技术有限公司
服务支持电话： 400-818-0055
电子邮箱： jiawei@cmgos.com

C&M Information Technologies Co., Ltd.
11F, Block C North Building, Raycom InfoTech Park, Beijing
mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人: Jia Wei <jiawei@cmgos.com>
发送时间: 2021 年 6 月 25 日 17:37
收件人: 吴毓杰 <win10sup@sdc.icbc.com.cn>
抄送: Jia Wei <jiawei@cmgos.com>
主题: [案例号: CAS-04372-M5F9L9] % |P3|ICBC|V0-H 升级 V2020-L 使用无线蓝屏 % 初次响应 CMIT:0001150

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 贾伟 。 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-04372-M5F9L9 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”**。

completely.The sender and ICBC are not responsible for the loss caused possibly by e-mail.