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：

用户使用计算机过程中蓝屏，已开启 NBL tracing。

案例进展：

和用户确认按照建议操作后蓝屏问题未再出现，可归档案例。

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 12 月 1 日 11:33
收件人: '吴毓杰' <win10sup@sdc.icbc.com.cn>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: [案例号: CAS-05162-T6S1S9] % |P2|ICBC|工行蓝屏 NBL 问题分析 % 初次响应 CMIT:0001194

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 11 月 26 日 17:11
收件人: '吴毓杰' <win10sup@sdc.icbc.com.cn>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: [案例号: CAS-05162-T6S1S9] % |P2|ICBC|工行蓝屏 NBL 问题分析 % 初次响应 CMIT:0001194

吴先生，您好

很高兴与您电话沟通，根据刚刚电话沟通的结果：此 dump 是由于 PTE 结构损坏导致的。对于 PTE 损坏的问题， 操作系统是没有办法直接跟踪的，所以只能通过收取多个日志来推测可能性原因。

建议操作：

1）硬件方面：查看现有 BIOS 和 Firmware 版本，并进行升级；

2）可以删除或者升级如下 filter driver 的组件：

TmPreFilter TmPreFlt 328500 Trend FSFilter Anti-Virus ffffc581b4d92ce0 4

vSelfSafe vSelfSafe_x64 385102 FSFilter Activity Monitor ffffc581b024a9d0 12

gscfmgr gscfmgr 369000 FSFilter Activity Monitor ffffc581ab319140 4

3）如果客户后续有新的 dump 生成，您可以回传后反馈此邮件。

日志分析：

==========
//bugcheck code 是 0x1a，原因是 0x41792 - 表示 PTE 损坏。
//从 crash stack 中，可以看到事情发生在 thread 退出的时候，清理相关内存的操作。

```
2: kd> !mex.crash
Dump Info
==========================================
Dump Name: MEMORY.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`3eaae000 PsLoadedModuleList = 0xfffff801`3eec4450
Debug session time: Mon Nov 22 16:06:14.150 2021 (UTC + 8:00)
System Uptime: 0 days 0:02:24.116
SystemManufacturer = LENOVO
SystemProductName = 20JTS2LF00
Processor: Intel(R) Core(TM) i5-6200U CPU @ 2.30GHz
Bugcheck: 1A (41792, FFFFED3FFE5F1290, 800000000, 0)
Kernel Complete Dump File: Full address space is available.


Bugcheck details
================================================
MEMORY_MANAGEMENT (1a)
   # Any other values for parameter 1 must be individually examined.
Arguments:
Arg1: 0000000000041792, A corrupt PTE has been detected. Parameter 2 contains the address
of
                the PTE. Parameters 3/4 contain the low/high parts of the PTE.
Arg2: ffffed3ffe5f1290
Arg3: 0000000800000000
Arg4: 0000000000000000

Crashing Stack
================================================
Process                Thread          CID       UserTime KernelTime ContextSwitches Wait
Reason   Time State
conhost.exe (ffffc581b9d64540) ffffc581b9d31080 57c.10ac        0s        0s             19
WrDispatchInt   0s Running on CPU 2

Priority:
   Current Base UB FB IO Page
   9       8    0  0  2  5

# Child-SP         Return           Call Site
 0 ffff8a0188fe6ba8 fffff8013ecc5d49 nt!KeBugCheckEx+0x0
 1 ffff8a0188fe6bb0 fffff8013eb6623e nt!MiDeleteVa+0x15b079
 2 ffff8a0188fe6cc0 fffff8013eb65da4 nt!MiWalkPageTablesRecursively+0x127e
 3 ffff8a0188fe6da0 fffff8013eb65da4 nt!MiWalkPageTablesRecursively+0xde4
 4 ffff8a0188fe6e80 fffff8013eb65da4 nt!MiWalkPageTablesRecursively+0xde4
 5 ffff8a0188fe6f60 fffff8013eb64c5a nt!MiWalkPageTablesRecursively+0xde4
 6 ffff8a0188fe7040 fffff8013eb674dd nt!MiWalkPageTables+0x1da
 7 ffff8a0188fe7140 fffff8013eb68035 nt!MiDeletePagablePteRange+0x1dd
```

```
 8 (Inline)         ---------------- nt!MiDeleteVirtualAddresses+0x41
 9 ffff8a0188fe7380 fffff8013f0926b1 nt!MiDeleteVad+0x7c5
 a ffff8a0188fe74f0 fffff8013f092298 nt!MiUnmapVad+0x49
 b ffff8a0188fe7520 fffff8013f09cff7 nt!MiCleanVad+0x30
 c ffff8a0188fe7550 fffff8013f0fe489 nt!MmCleanProcessAddressSpace+0x113
 d ffff8a0188fe75d0 fffff8013f0b221c nt!PspRundownSingleProcess+0x129
 e ffff8a0188fe7650 fffff8013f134f53 nt!PspExitThread+0x5c8
 f (Inline)         ---------------- nt!PsExitCurrentUserThread+0x14
10 ffff8a0188fe7750 fffff8013eb1ea30 nt!KiSchedulerApcTerminate+0x33
11 ffff8a0188fe7790 fffff8013ec6a240 nt!KiDeliverApc+0x470
12 ffff8a0188fe7850 fffff8013ec770af nt!KiInitiateUserApc+0x70
13 ffff8a0188fe7990 00007ffcc21a3364 nt!KiSystemServiceExit+0x9f
14 000000dd0007f9d8 0000000000000000 0x7ffcc21a3364

This thread is crashing
Warning!!! Thread is marked as terminated, but the termination has not completed. Could be
caused by disabling of APCs ?

2: kd> .frame /r 0x1; !mex.x
01 ffff8a01`88fe6bb0 fffff801`3eb6623e     nt!MiDeleteVa+0x15b079
[minkernel\ntos\mm\deleteva.c @ 2423]
rax=0000000000000000 rbx=0000000800000000 rcx=000000000000001a
rdx=0000000000041792 rsi=ffffed3ffe5f1290 rdi=ffff8a0188fe71b0
rip=fffff8013ecc5d49 rsp=ffff8a0188fe6bb0 rbp=ffff8a0188fe6c59
r8=ffffed3ffe5f1290  r9=0000000800000000 r10=0000000000000000
r11=ffffc581b9d64a40 r12=00007ffcbe252000 r13=0000000000000042
r14=ffff8a0188fe7260 r15=ffff8a0188fe7170
iopl=0         nv up ei pl zr na po nc
cs=0010  ss=0018  ds=002b  es=002b  fs=0053  gs=002b             efl=00000246
nt!MiDeleteVa+0x15b079:
fffff801`3ecc5d49 cc              int     3
@rdi             PageTableWalk = 0xffff8a01`88fe71b0
@rsi             PointerPte = 0xffffed3f`fe5f1290
ffff8a01`88fe6bf8 PagingLevel = MiPteLevel (0n0)
<unavailable>     ProtoPte = <value unavailable>
@r12             Va = 0x00007ffc`be252000
<unavailable>     DeleteResult = <value unavailable>
<unavailable>     Pfn1 = <value unavailable>
ffff8a01`88fe6c0c PteMadeZero = 0
<unavailable>     PageFrameIndex = <value unavailable>
ffff8a01`88fe6be8 PteContents = struct _MMPTE
@rbx             Vm = 0x00000008`00000000
@r13d             DeleteFlags = 0x42
<unavailable>     PageTableEmpty = <value unavailable>
@r14             TbFlushList = 0xffff8a01`88fe7260
```

```
@r15             DeleteVaInfo = 0xffff8a01`88fe7170
<unavailable>    NumberOfTranslations = <value unavailable>
ffff8a01`88fe6c48 IoPageFrame = 0xffffed76`9fff2f80
<unavailable>    CloneDescriptor = <value unavailable>
```

//发现当前的 PTE 的结构有损坏

```
2: kd> !pte 0xffffed3f`fe5f1290
                                           VA 00007ffcbe252000
PXE at FFFFED76BB5DA7F8    PPE at FFFFED76BB4FFF90    PDE at FFFFED769FFF2F88    PTE at
FFFFED3FFE5F1290
contains 0A00000106CB7867  contains 0A0000010BFFA867  contains
1A0000010C0CB867  contains 0000000800000000
pfn 106cb7    ---DA--UWEV  pfn 10bffa    ---DA--UWEV  pfn 10c0cb    ---DA--UWEV  not
valid
                                                      Page has been freed
```

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 11 月 24 日 10:44
收件人: 吴毓杰 <win10sup@sdc.icbc.com.cn>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: [案例号: CAS-05162-T6S1S9] % |P2|ICBC|工行蓝屏 NBL 问题分析 % 初次响应 CMIT:0001194

吴先生, 您好!

收到您上传的 2 个 dump 文件。

一、**MEMORY.DMP** 的 Call stack 与之前处理的 vwifimf.sys 问题不一致，请确认这台机器出现蓝屏问题时的具体操作。

二、**wangyifeng.DMP** 分析结果和之前原因一致，建议排查 vwifimf.sys。但我在运行需要 NBL Tracing 相关命令时遇到如下提示:

```
0: kd> !ndiskd.nbllog
    This command requires NBL tracking to be enabled on the debugee target
    machine.  (By default, client operating systems have level 2, and servers
    have level 0).  To enable, set this REG_DWORD value to a nonzero value on
    the target machine and reboot the target machine:

    HKLM\SYSTEM\CurrentControlSet\Services\NDIS\Parameters ! TrackNblOwner
    Possible Values (features are cumulative)
    * 0:  Disable all tracking.
    * 1:  Track the most recent owner of each NBL (enables !ndiskd.pendingnbls)
    * 2:  Scan for leaks at runtime (use with StuckNblReaction)
    * 3:  Keep a full history of all activity (enables !ndiskd.nbllog and
    !ndiskd.nbl -log)
    * 4:  Take stack capture snapshots (slow, but enables !ndiskd.nbl -log
    -stacks)
    This command requires level 3 or higher.
```

还请确认 HKLM\SYSTEM\CurrentControlSet\Services\NDIS\Parameters 界面 TrackNblOwner 是否设置成功。可反馈截图给我进行确认，如果没有设置成功请以管理员身份运行命令提示符，运行如下命令：

reg add "HKLM\SYSTEM\CurrentControlSet\Services\NDIS\Parameters" /t REG_DWORD /v TrackNblOwner /d 4 /f

wangyifeng.DMP 分析过程：

```
0: kd> .frame /r 06
06 fffff802`11478d40
fffff802`18b9d66d     nwifi!Dot11SendCompletion+0x4b
rax=ffffe7017e45c050 rbx=ffffe70188531d30 rcx=ffffe70195aa1d30
rdx=0000000000000000 rsi=ffffe70195aa1d30 rdi=ffffe701876e0790
rip=fffff80218b99513 rsp=fffff80211478d40 rbp=0000000000000000
r8=ffffe701852ae2c0  r9=ffffe7017e769010 r10=0000000000000001
r11=ffffe70195c109c0 r12=ffffe7017a261920 r13=ffffe70183cbd060
r14=ffffe701817a8658 r15=ffffe701839c5c00
iopl=0         nv up ei pl zr na po nc
cs=0010  ss=0018  ds=002b  es=002b  fs=0053  gs=002b
efl=00000246
nwifi!Dot11SendCompletion+0x4b:
fffff802`18b99513 4883eb18        sub     rbx,18h


0: kd> dt ffffe70195aa1d30 nwifi!_NET_BUFFER_LIST
 NET_BUFFER_LIST
   +0x000 Next             : (null)
   +0x008 FirstNetBuffer   : 0xffffe701`95aa1eb0  _NET_BUFFER
   +0x000 Link             : _SLIST_HEADER
   +0x000 NetBufferListHeader : _NET_BUFFER_LIST_HEADER
```

```
   +0x010 Context          : 0xffffe701`876e0750
_NET_BUFFER_LIST_CONTEXT
   +0x018 ParentNetBufferList : (null)
   +0x020 NdisPoolHandle   : 0xffffe701`83c89040 Void
   +0x030 NdisReserved     : [2] (null)
   +0x040 ProtocolReserved : [4] 0xffffe701`960799c0 Void
   +0x060 MiniportReserved : [2] (null)
   +0x070 Scratch          : (null)
   +0x078 SourceHandle     : 0xffffe701`83cb38a0 Void
   +0x080 NblFlags         : 0
   +0x084 ChildRefCount    : 0n0
   +0x088 Flags            : 0x500
   +0x08c Status           : 0n0
   +0x08c NdisReserved2    : 0
   +0x090 NetBufferListInfo : [26] (null)


0: kd> !pool 0xffffe701`83c89040
Pool page ffffe70183c89040 region is Nonpaged pool
*ffffe70183c89000 size:  a00 previous size:    0  (Allocated)
*Filt
              Owning component : Unknown (update pooltag.txt)
ffffe70183c89a10 size:  270 previous
size:    0  (Allocated)  Ntfn
ffffe70183c89ca0 size:  270 previous
size:    0  (Allocated)  Ntfn
ffffe70183c89f10 size:   d0 previous
size:    0  (Free)       ...X


0: kd> !mex.tag Filt
Name    Number of Hits Version Time Stamp          Location
======= ============== ======= ==================
=======================================
vwifimf              1 0.0.0.0 08/05/2021 13:00:35
\SystemRoot\system32\DRIVERS\vwifimf.sys

Hits
=============================================
fffff802`15601790  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 <jiawei@cmgos.com>
发送时间: 2021 年 11 月 23 日 17:30
收件人: 吴毓杰 <win10sup@sdc.icbc.com.cn>
抄送: Jia Wei <jiawei@cmgos.com>
主题: [案例号: CAS-05162-T6S1S9] % |P2|ICBC|工行蓝屏 NBL 问题分析 % 初次响应 CMIT:0001194

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-05162-T6S1S9 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
