<https://hsdes.intel.com/appstore/article/#/14018150675>

[Win11 OS][HLK][SV2][NetCx][WWAN]DPC\_WATCHDOG\_VIOLATION (133) in MbbCx during NDISTest GenericMiniportRequirements execution:

the scope of request manager spinlock has been changed in MbbReqFsmCancelled and, as a result, second call to the MbbReqMgrDerefRequest is done with request manager’s spinlock acquired.  But since MbbReqMgrDerefRequest attempts to acquire request manager’s spinlock again, this leads to deadlock:

**8: kd> !analyze -show**

**DPC\_WATCHDOG\_VIOLATION (133)**

**The DPC watchdog detected a prolonged run time at an IRQL of DISPATCH\_LEVEL**

**or above.**

**Arguments:**

**Arg1: 0000000000000001, The system cumulatively spent an extended period of time at**

**DISPATCH\_LEVEL or above.**

**Arg2: 0000000000001e00, The watchdog period (in ticks).**

**Arg3: fffff8021b1553f0, cast to nt!DPC\_WATCHDOG\_GLOBAL\_TRIAGE\_BLOCK, which contains**

**additional information regarding the cumulative timeout**

**Arg4: 0000000000000000**

**8: kd> k**

**# Child-SP          RetAddr               Call Site**

**00 ffffb301`57c6cc78 fffff802`1a6ed755     nt!KeBugCheckEx**

**01 ffffb301`57c6cc80 fffff802`1a6ec3d4     nt!KeAccumulateTicks+0x475**

**02 ffffb301`57c6cd10 fffff802`1a6e73a3     nt!KiUpdateRunTime+0xf4**

**03 ffffb301`57c6ce90 fffff802`1a6e68f9     nt!KeClockInterruptNotify+0x763**

**04 ffffb301`57c6cf40 fffff802`1a7572cc     nt!HalpTimerClockInterrupt+0x109**

**05 ffffb301`57c6cf70 fffff802`1a87c37a     nt!KiCallInterruptServiceRoutine+0x9c**

**06 ffffb301`57c6cfb0 fffff802`1a87c94c     nt!KiInterruptSubDispatchNoLockNoEtw+0xfa**

**07 ffff8409`d348f610 fffff802`1a686eac     nt!KiInterruptDispatchNoLockNoEtw+0x3c**

**08 ffff8409`d348f7a0 fffff802`1a686e7e     nt!KxWaitForSpinLockAndAcquire+0x1c**

**09 ffff8409`d348f7d0 fffff802`1aa1d018     nt!KeAcquireSpinLockRaiseToDpc+0x8e**

**0a ffff8409`d348f800 fffff802`1af064c2     nt!DifKeAcquireSpinLockRaiseToDpcWrapper+0xb8**

**0b ffff8409`d348f850 fffff802`e5a5b4c7     nt!VerifierKeAcquireSpinLockRaiseToDpc+0x32**

**0c ffff8409`d348f880 fffff802`e5a5c52c     MbbCx!MbbReqMgrLockManager+0x17**

**0d ffff8409`d348f8b0 fffff802`e5a5de1f     MbbCx!MbbReqMgrDerefRequest+0x64**

**0e ffff8409`d348f8f0 fffff802`e5a5ce52     MbbCx!MbbReqFsmCancelled+0x1bf**

**0f (Inline Function) --------`--------     MbbCx!MbbReqMgrTransition+0xa6**

**10 ffff8409`d348f930 fffff802`e5a5c94c     MbbCx!MbbReqMgrQueueEvent+0x18e**

**11 ffff8409`d348f9a0 fffff802`e5a5cb48     MbbCx!MbxMessageCancelRequestsHandler+0x2ac**

**12 ffff8409`d348fa70 fffff802`e5a5ff70     MbbCx!MbxMessagesHandler+0x88**

**13 ffff8409`d348fac0 fffff802`1a62e7c7     MbbCx!MbbWorkMgrProcessWorkItem+0x120**

**14 ffff8409`d348fb30 fffff802`1a87b364     nt!PspSystemThreadStartup+0x57**

**15 ffff8409`d348fb80 00000000`00000000     nt!KiStartSystemThread+0x34**

**8: kd> .frame /r c**

**0c ffff8409`d348f880 fffff802`e5a5c52c     MbbCx!MbbReqMgrLockManager+0x17**

**rax=0000000000000001 rbx=ffffe7824cbe0c00 rcx=ffffe7824cbe0cb0**

**rdx=fffff802e5a5b4c7 rsi=0000000000000000 rdi=ffffe7824ac19610**

**rip=fffff802e5a5b4c7 rsp=ffff8409d348f880 rbp=0000000000000006**

**r8=fffff802e5a5b4c7  r9=00007ffffffeffff r10=fffff8021b6e5b70**

**r11=0000000000000000 r12=fffff802e5a30000 r13=fffff802e5a86f50**

**r14=ffffe7824cbe0c00 r15=fffff802e5a86f50**

**iopl=0         nv up ei pl zr na po nc**

**cs=0010  ss=0018  ds=002b  es=002b  fs=0053  gs=002b             efl=00000246**

**MbbCx!MbbReqMgrLockManager+0x17:**

**fffff802`e5a5b4c7 0f1f440000      nop     dword ptr [rax+rax]**

**8: kd> ub**

**MbbCx!MbbReqMgrGetRequestByKey+0x5d:**

**fffff802`e5a5b4ad cc              int     3**

**fffff802`e5a5b4ae cc              int     3**

**fffff802`e5a5b4af cc              int     3**

**MbbCx!MbbReqMgrLockManager:**

**fffff802`e5a5b4b0 4053            push    rbx**

**fffff802`e5a5b4b2 4883ec20        sub     rsp,20h**

**fffff802`e5a5b4b6 488bd9          mov     rbx,rcx**

**fffff802`e5a5b4b9 4881c1b0000000  add     rcx,0B0h**

**fffff802`e5a5b4c0 48ff15c1fe0200  call    qword ptr [MbbCx!\_imp\_KeAcquireSpinLockRaiseToDpc (fffff802`e5a8b388)]**

**8: kd> dv /V /i /t**

**prv param  @rbx              @rbx              struct \_MBB\_REQUEST\_MANAGER \* RequestManager = 0xffffe782`4cbe0c00**

**8: kd> dt \_MBB\_REQUEST\_MANAGER  0xffffe782`4cbe0c00 SpinLock.SpinLock**

**MbbCx!\_MBB\_REQUEST\_MANAGER**

**+0x0b0 Spinlock          :**

**+0x000 SpinLock          : 1**

<https://hsdes.intel.com/appstore/article/#/22016256678>

(WIFI-267972)[WIN11][SV2][NetAdapter] OS doesn't trigger surprise removal causing BSOD 0x9F:

This is Bugcheck 9F - DRIVER\_POWER\_STATE\_FAILURE (9f)

2: kd> !Analyze -v;

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*                                                                             \*

\*                        Bugcheck Analysis                                    \*

\*                                                                             \*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

DRIVER\_POWER\_STATE\_FAILURE (9f)

A driver has failed to complete a power IRP within a specific time.

Arguments:

Arg1: 0000000000000003, A device object has been blocking an IRP for too long a time

Arg2: ffff9c8884de9060, Physical Device Object of the stack

Arg3: fffffd86c1a5f718, nt!TRIAGE\_9F\_POWER on Win7 and higher, otherwise the Functional Device Object of the stack

Arg4: ffff9c888a30d9b0, The blocked IRP

2: kd> !irp ffff9c888a30d9b0

Irp is active with 8 stacks 6 is current (= 0xffff9c888a30dbe8)

 No Mdl: No System Buffer: Thread 00000000:  Irp stack trace.  Pending has been returned

     cmd  flg cl Device   File     Completion-Context

 [N/A(0), N/A(0)]

            0  0 00000000 00000000 00000000-00000000

Args: 00000000 00000000 00000000 00000000

 [N/A(0), N/A(0)]

            0  0 00000000 00000000 00000000-00000000

Args: 00000000 00000000 00000000 00000000

 [N/A(0), N/A(0)]

            0  0 00000000 00000000 00000000-00000000

Args: 00000000 00000000 00000000 00000000

 [N/A(0), N/A(0)]

            0  0 00000000 00000000 00000000-00000000

Args: 00000000 00000000 00000000 00000000

 [IRP\_MJ\_POWER(16), IRP\_MN\_SET\_POWER(2)]

            0 e1 ffff9c8884de9060 00000000 00000000-00000000    pending

       \Driver\pci

Args: 00041100 00000001 00000001 00000002

>[IRP\_MJ\_POWER(16), IRP\_MN\_SET\_POWER(2)]

            0 e1 ffff9c8883f3bde0 00000000 fffff8077f9c5a60-ffff9c887deba8b0 Success Error Cancel pending

       \Driver\Netwaw12 MSDMFilt!MsdmFiltPower\_CompletionRoutine

Args: 00041100 00000001 00000001 00000002

 [IRP\_MJ\_POWER(16), IRP\_MN\_SET\_POWER(2)]

            0 e1 ffff9c887deba760 00000000 fffff8077e1a7c10-ffff9c888a96ad30 Success Error Cancel pending

       \Driver\MSDMFilt nt!PopRequestCompletion

Args: 00041100 00000001 00000001 00000002

2: kd>  !devstack ffff9c8883f3bde0

  !DevObj           !DrvObj            !DevExt           ObjectName

  ffff9c887deba760  \Driver\MSDMFilt   ffff9c887deba8b0

> ffff9c8883f3bde0  \Driver\Netwaw12   ffff9c8882931f20

  ffff9c887f3d1b10  \Driver\ACPI       ffff9c8885065a90

  ffff9c8884de9060  \Driver\pci        ffff9c8884de91b0  NTPNP\_PCI0020

!DevNode ffff9c8876cb82b0 :

  DeviceInst is "PCI\VEN\_8086&DEV\_272B&SUBSYS\_00F08086&REV\_1A\4&2980c731&0&00E0"

  ServiceName is "Netwaw12"

KMDF is waiting for the power event processing to start self-managed I/O:

2: kd>  !wdfkd.wdfdriverinfo Netwaw12

----------------------------------

Default driver image name: Netwaw12

WDF library image name: Wdf01000

 FxDriverGlobals  0xffff9c88857f02a0

 WdfBindInfo      0xfffff8053a835660

   Version        v1.31

 Library module   0xffff9c886f7e2e40

   ServiceName    \Registry\Machine\System\CurrentControlSet\Services\Wdf01000

   ImageName      Wdf01000

----------------------------------

WDFDRIVER: 0x0000637774d2cf78

Driver logs: Not available

Framework logs: !wdflogdump Netwaw12.sys -f

    !wdfdevice 0x000063777d6ce3c8 ff (FDO)

2: kd> !wdfdevice 0x000063777d6ce3c8 ff

Treating handle as a KMDF handle!

Dumping WDFDEVICE 0x000063777d6ce3c8

=================================

WDM PDEVICE\_OBJECTs: self 0x83F3BDE0 attached 0x7F3D1B10 pdo 0x84DE9060

Pnp state:  129 ( WdfDevStatePnpFailedIoStarting )

Power state:  32b ( WdfDevStatePowerStartSelfManagedIo )

Power Pol state:  525 ( WdfDevStatePwrPolSystemWakeDeviceWakeCompletePowerUp )

Default WDFIOTARGET: 000063777cd5fc48

Self    WDFIOTARGET: 000063777cd5fa98

Device is the power policy owner for the stack

No pended wait-wake irps

Pended pnp(IRP\_MN\_SURPRISE\_REMOVAL) !irp 0xffff9c887f5abaa0

Pended device power !irp 0xffff9c888a30d9b0 (D0)

Pnp state history:

[0] WdfDevStatePnpObjectCreated (0x100)

[1] WdfDevStatePnpInit (0x105)

[2] WdfDevStatePnpInitStarting (0x106)

[3] WdfDevStatePnpHardwareAvailable (0x108)

[4] WdfDevStatePnpEnableInterfaces (0x109)

[5] WdfDevStatePnpStarted (0x119)

[6] WdfDevStatePnpSurpriseRemoveIoStarted (0x127)

[7] WdfDevStatePnpFailedIoStarting (0x129)

owning thread:  ffff9c887ffa1040

Power state history:

[0] WdfDevStatePowerDx (0x31f)

[1] WdfDevStatePowerCheckDeviceType (0x301)

[2] WdfDevStatePowerWaking (0x333)

[3] WdfDevStatePowerNotifyingD0EntryToWakeInterrupts (0x35a)

[4] WdfDevStatePowerWakingConnectInterrupt (0x335)

[5] WdfDevStatePowerWakingDmaEnable (0x339)

[6] WdfDevStatePowerWakingPostHardwareEnabled (0x363)

[7] WdfDevStatePowerStartSelfManagedIo (0x32b)

2: kd> !thread ffff9c887ffa1040

THREAD ffff9c887ffa1040  Cid 0004.0488  Teb: 0000000000000000 Win32Thread: 0000000000000000 WAIT: (Executive) KernelMode Non-Alertable

    fffffd86c5c3f2b8  SynchronizationEvent

Not impersonating

DeviceMap                 ffffd2828d806c80

Owning Process            ffff9c886f0f2040       Image:         System

Attached Process          N/A            Image:         N/A

Wait Start TickCount      846694         Ticks: 7549 (0:00:01:57.953)

Context Switch Count      68893          IdealProcessor: 0  NoStackSwap

UserTime                  00:00:00.000

KernelTime                00:00:09.031

Win32 Start Address nt!ExpWorkerThread (0xfffff8077e016e40)

Stack Init fffffd86c5c3fb70 Current fffffd86c5c3ea80

Base fffffd86c5c40000 Limit fffffd86c5c39000 Call 0000000000000000

Priority 12 BasePriority 12 PriorityDecrement 0 IoPriority 2 PagePriority 5

Child-SP          RetAddr               : Args to Child                                                           : Call Site

fffffd86`c5c3eac0 fffff807`7e0c8e65     : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : nt!KiSwapContext+0x76

fffffd86`c5c3ec00 fffff807`7e0ca287     : ffff9c88`7ffa1040 ffff9c88`00000000 ffff9c88`920fe000 00000000`00000000 : nt!KiSwapThread+0xb05

fffffd86`c5c3ed50 fffff807`7e0cc8d6     : 000004f0`00000000 00000000`00000001 000004f0`00000000 00000000`00000000 : nt!KiCommitThreadWait+0x137

fffffd86`c5c3ee00 fffff807`7e3d6793     : fffff805`3a9952d9 00000000`00000000 00000000`0000000d ffff9c88`6f0a8530 : nt!KeWaitForSingleObject+0x256

fffffd86`c5c3f1a0 fffff807`7e8b1593     : ffff9c88`7f498c00 00000000`00000000 00006377`7d055800 00000000`00000001 : nt!DifKeWaitForSingleObjectWrapper+0xf3

fffffd86`c5c3f230 fffff805`3a9952d9     : ffff9c88`7f498cf0 00000000`00000001 00006377`79ae43a8 00000000`0000002b : nt!VerifierKeWaitForSingleObject+0x53

(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : NetAdapterCx!KWaitEventBase<wistd::integral\_constant<enum \_EVENT\_TYPE,1> >::Wait+0x24 (Inline Function @ fffff805`3a9952d9) [onecore\internal\minwin\priv\_sdk\inc\net\ndis\rtl\kwaitevent.h @ 64]

fffffd86`c5c3f270 fffff805`3a99e8a9     : 00006377`79ae43a8 fffffd86`c5c3f340 00000000`00000004 00000000`00000000 : NetAdapterCx!AdapterPnpPower::NetAdapterStop+0xdd [minio\netcx\adapter\adapterpnppower.cpp @ 223]

(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : NetAdapterCx!AdapterPnpPower::NetAdapterStop+0x13 (Inline Function @ fffff805`3a99e8a9) [minio\netcx\adapter\adapterpnppower.cpp @ 203]

fffffd86`c5c3f2e0 fffff805`44769617     : 00000000`00000000 00006377`79ae43a8 ffff9c88`8699b070 ffff9c88`8699b068 : NetAdapterCx!imp\_NetAdapterStop+0x59 [minio\netcx\adapter\nxadapterapi.cpp @ 386]

fffffd86`c5c3f310 fffff805`4476992f     : fffff805`447991a0 00000000`00000000 00000000`00000000 ffff9c88`89e43ba0 : WifiCx!WxDevice::DeleteInnerPort+0xeb

fffffd86`c5c3f380 fffff805`44769c92     : 00000000`00000005 ffff9c88`8699b030 00000000`00000002 fffff807`7e8b14b3 : WifiCx!WxDevice::DeletePortTypes+0x233

fffffd86`c5c3f400 fffff805`44767b65     : 00000000`00000005 00000000`0000000c 00000000`00000001 ffff9c88`8699b030 : WifiCx!WxDevice::PostSelfManagedIoSuspendEx+0xde

fffffd86`c5c3f460 fffff807`7f55d66d     : ffff9c88`8ba02c60 00000000`00000000 00000000`00000004 ffff9c88`857f02a0 : WifiCx!EvtCxDevicePostSelfManagedIoSuspendEx+0x55

fffffd86`c5c3f490 fffff807`7f569ac4     : ffff9c88`8ba02c60 00000000`00000000 fffffd86`c5c3000c fffffd86`c5c3f5a8 : Wdf01000!FxPnpDeviceSelfManagedIoSuspend::InvokeCxCallback+0x5d [minkernel\wdf\framework\shared\irphandlers\pnp\pnpcallbacks.cpp @ 988]

fffffd86`c5c3f4f0 fffff807`7f4fff17     : ffff9c88`7f0a1a28 ffff9c88`82931c30 00000000`00000000 fffffd86`c5c3f5c0 : Wdf01000!FxPrePostCallback::IssuePostCxCallbacks+0x54 [minkernel\wdf\framework\shared\irphandlers\pnp\cxpnppowercallbacks.cpp @ 513]

fffffd86`c5c3f520 fffff807`7f571c1e     : ffff9c88`7f0a19b0 ffff9c88`7f0a1a80 fffff807`7f57d900 fffff807`7f580220 : Wdf01000!FxPrePostCallback::InvokeStateless+0x5f [minkernel\wdf\framework\shared\irphandlers\pnp\cxpnppowercallbacks.cpp @ 423]

(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : Wdf01000!FxPnpDeviceSelfManagedIoSuspend::Invoke+0xc (Inline Function @ fffff807`7f571c1e) [minkernel\wdf\framework\shared\irphandlers\pnp\pnpcallbacks.cpp @ 888]

fffffd86`c5c3f550 fffff807`7f571b99     : ffff9c88`7f0a19b0 00000000`0000000c ffff9c88`7f0a1a80 fffff807`7f57de00 : Wdf01000!FxSelfManagedIoMachine::RestartedFailedPost+0x2e [minkernel\wdf\framework\shared\irphandlers\pnp\selfmanagediostatemachine.cpp @ 625]

fffffd86`c5c3f580 fffff807`7f55fd29     : ffff9c88`76c9f8b0 00000000`c0000001 fffffd86`c5c3f720 fffff807`7f57de60 : Wdf01000!FxSelfManagedIoMachine::ProcessEvent+0x149 [minkernel\wdf\framework\shared\irphandlers\pnp\selfmanagediostatemachine.cpp @ 339]

(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : Wdf01000!FxSelfManagedIoMachine::Start+0x14 (Inline Function @ fffff807`7f55fd29) [minkernel\wdf\framework\shared\inc\private\common\FxSelfManagedIoStateMachine.hpp @ 138]

fffffd86`c5c3f5f0 fffff807`7f55e970     : ffff9c88`76c9f802 fffffd86`c5c3f720 00000000`00000c60 00000000`00000000 : Wdf01000!FxPkgPnp::PowerStartSelfManagedIo+0x39 [minkernel\wdf\framework\shared\irphandlers\pnp\powerstatemachine.cpp @ 3318]

fffffd86`c5c3f620 fffff807`7f55f947     : fffff807`7e0fa7a0 fffff807`7f571570 00000000`00000800 00000000`00000c60 : Wdf01000!FxPkgPnp::PowerEnterNewState+0x194 [minkernel\wdf\framework\shared\irphandlers\pnp\powerstatemachine.cpp @ 1699]

fffffd86`c5c3f760 fffff807`7f560922     : fffffd86`c5c3f830 00000000`00000000 ffff9c88`76c9fab8 ffff9c88`7ffa1040 : Wdf01000!FxPkgPnp::PowerProcessEventInner+0x177 [minkernel\wdf\framework\shared\irphandlers\pnp\powerstatemachine.cpp @ 1613]

fffffd86`c5c3f7e0 fffff807`7f571271     : ffff9c88`76c9fab0 ffff9c88`76c9fa90 00000000`00000000 00000000`00000000 : Wdf01000!FxPkgPnp::\_PowerProcessEventInner+0x32 [minkernel\wdf\framework\shared\irphandlers\pnp\powerstatemachine.cpp @ 1447]

fffffd86`c5c3f810 fffff807`7f57157c     : ffff9c88`80137210 ffff9c88`83f3bde0 ffff9c88`00000000 00000000`00000001 : Wdf01000!FxEventQueue::EventQueueWorker+0x75 [minkernel\wdf\framework\shared\irphandlers\pnp\eventqueue.cpp @ 279]

fffffd86`c5c3f860 fffff807`7e0fa8a0     : 00000000`00000000 ffff9c88`767e5060 00000000`00000000 ffff9c88`767e5060 : Wdf01000!FxThreadedEventQueue::\_WorkItemCallback+0xc [minkernel\wdf\framework\shared\irphandlers\pnp\eventqueue.cpp @ 437]

fffffd86`c5c3f890 fffff807`7e016f95     : ffff9c88`6f136c50 ffff9c88`7ffa1040 fffffd86`c5c3fa00 25252525`00000000 : nt!IopProcessWorkItem+0x100

fffffd86`c5c3f900 fffff807`7e10a8b7     : ffff9c88`7ffa1040 00000000`0000029a ffff9c88`7ffa1040 fffff807`7e016e40 : nt!ExpWorkerThread+0x155

fffffd86`c5c3faf0 fffff807`7e22f324     : fffff807`7c3f1180 ffff9c88`7ffa1040 fffff807`7e10a860 25252525`25252525 : nt!PspSystemThreadStartup+0x57

fffffd86`c5c3fb40 00000000`00000000     : fffffd86`c5c40000 fffffd86`c5c39000 00000000`00000000 00000000`00000000 : nt!KiStartSystemThread+0x34

But the Power Machine is also waiting:

2: kd> !thread  ffff9c888e632040

THREAD ffff9c888e632040  Cid 0004.3130  Teb: 0000000000000000 Win32Thread: 0000000000000000 WAIT: (Executive) KernelMode Non-Alertable

    ffff9c888640ecc0  NotificationEvent

Not impersonating

DeviceMap                 ffffd2828d806c80

Owning Process            ffff9c886f0f2040       Image:         System

Attached Process          N/A            Image:         N/A

Wait Start TickCount      846693         Ticks: 7550 (0:00:01:57.968)

Context Switch Count      1032           IdealProcessor: 0  NoStackSwap

UserTime                  00:00:00.000

KernelTime                00:00:00.421

Win32 Start Address nt!ExpWorkerThread (0xfffff8077e016e40)

Stack Init fffffd86c3157b70 Current fffffd86c3156c60

Base fffffd86c3158000 Limit fffffd86c3151000 Call 0000000000000000

Priority 13 BasePriority 12 PriorityDecrement 0 IoPriority 2 PagePriority 5

Child-SP          RetAddr               : Args to Child                                                           : Call Site

fffffd86`c3156ca0 fffff807`7e0c8e65     : 00000000`00000001 00000000`00000000 ffff9c88`8020d030 fffffd86`c31575f0 : nt!KiSwapContext+0x76

fffffd86`c3156de0 fffff807`7e0ca287     : ffff9c88`8e632040 ffff9c88`00000000 00000000`00000000 00000000`00000000 : nt!KiSwapThread+0xb05

fffffd86`c3156f30 fffff807`7e0cc8d6     : 00000000`00000000 00000000`00000001 00000000`00000000 00000000`00000000 : nt!KiCommitThreadWait+0x137

fffffd86`c3156fe0 fffff807`7f50675e     : 00000000`5270784e 00000000`00000103 00006377`7d6ce301 00000000`00000000 : nt!KeWaitForSingleObject+0x256

(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : Wdf01000!MxEvent::WaitFor+0x1c (Inline Function @ fffff807`7f50675e) [minkernel\wdf\framework\shared\inc\primitives\km\MxEventKm.h @ 122]

(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : Wdf01000!FxCREvent::EnterCRAndWait+0x28 (Inline Function @ fffff807`7f50675e) [minkernel\wdf\framework\shared\inc\private\common\FxWaitLock.hpp @ 79]

(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : Wdf01000!FxCREvent::EnterCRAndWaitAndLeave+0x28 (Inline Function @ fffff807`7f50675e) [minkernel\wdf\framework\shared\inc\private\common\FxWaitLock.hpp @ 93]

(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : Wdf01000!FxPowerIdleMachine::WaitForD0+0x28 (Inline Function @ fffff807`7f50675e) [minkernel\wdf\framework\shared\inc\private\common\FxPowerIdleStateMachine.hpp @ 188]

fffffd86`c3157380 fffff807`7f521629     : 00000000`00000002 00000000`5270784e 00000000`00000001 fffff807`7e0cea08 : Wdf01000!FxPowerIdleMachine::PowerReferenceWorker+0xddc6 [minkernel\wdf\framework\shared\irphandlers\pnp\poweridlestatemachine.cpp @ 1576]

(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : Wdf01000!FxPowerIdleMachine::PowerReference+0x2e (Inline Function @ fffff807`7f521629) [minkernel\wdf\framework\shared\inc\private\common\FxPowerIdleStateMachine.hpp @ 200]

(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : Wdf01000!FxPkgPnp::PowerReference+0x33 (Inline Function @ fffff807`7f521629) [minkernel\wdf\framework\shared\inc\private\common\FxPkgPnp.hpp @ 3884]

fffffd86`c31573f0 fffff807`7f5238fb     : ffff9c88`82931c30 ffff9c88`7cd96fc0 00000000`00000001 ffff9c88`8020d000 : Wdf01000!StopIdleWorker+0xe5 [minkernel\wdf\framework\shared\core\fxdeviceapi.cpp @ 1354]

fffffd86`c3157440 fffff805`3a9c5f8b     : 00000000`00000005 fffff807`7e00ee72 00000000`00000002 ffff9c88`6f0b8078 : Wdf01000!imp\_WdfDeviceStopIdleActual+0x1b [minkernel\wdf\framework\shared\core\fxdeviceapi.cpp @ 1501]

(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : NetAdapterCx!WdfDeviceStopIdleActual+0x35 (Inline Function @ fffff805`3a9c5f8b) [onecore\external\ddk\inc\wdf\kmdf\1.31\wdfdevice.h @ 4198]

fffffd86`c3157480 fffff805`3a99a78e     : ffff9c88`8a5f29b0 ffff9c88`6f0a8530 ffff9c88`6f0b8068 fffff807`7e8c6ca1 : NetAdapterCx!NxPowerReference::PowerReference+0x97 [minio\netcx\adapter\powerpolicy\nxpowerreference.cpp @ 114]

(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : NetAdapterCx!NxPowerPolicy::PowerReference+0x5 (Inline Function @ fffff805`3a99a78e) [minio\netcx\adapter\powerpolicy\nxpowerpolicy.cpp @ 1067]

(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : NetAdapterCx!NxAdapter::PowerReference+0x5 (Inline Function @ fffff805`3a99a78e) [minio\netcx\adapter\nxadapter.cpp @ 4176]

fffffd86`c31574d0 fffff807`8026e59c     : ffff9c88`8a5f29b0 ffff9c88`8a5f2ac0 00000000`00000080 fffff807`7e8b14b3 : NetAdapterCx!EvtNdisPowerReference+0x6e [minio\netcx\adapter\nxadapter.cpp @ 1573]

fffffd86`c3157500 fffff807`802dd955     : ffff9c88`8a5f29b0 00000000`00000001 ffff9c88`8020d030 ffff9c88`8020d030 : ndis!ndisWdfAcquirePowerReferenceHelper+0x30

fffffd86`c3157550 fffff807`80280538     : ffff9c88`8020d030 00000000`00000001 fffff807`80323048 00000000`00000000 : ndis!ndisSelectiveSuspendStop+0x25d

fffffd86`c31575c0 fffff807`80363e30     : ffff9c88`8020d030 00000000`00000001 fffff807`80323048 00000000`00000000 : ndis!ndisPowerSaveStop+0x384f0

fffffd86`c31575f0 fffff807`802aef23     : ffff9c88`8020d030 ffff9c88`8020d030 00000000`00000000 00000000`00000000 : ndis!ndisPnPIrpSurpriseRemovalInner+0x84

fffffd86`c31576f0 fffff807`8028fa80     : 00000000`00000000 00000000`00000000 00000000`00000000 ffff9c88`8020d030 : ndis!ndisPnPIrpSurpriseRemoval+0x14f

fffffd86`c3157740 fffff805`3a995962     : ffff9c88`915e4be0 fffff805`3a9b4100 ffff9c88`915e4be0 fffff807`7e8b16d1 : ndis!NdisWdfPnpPowerEventHandler+0xc0

(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : NetAdapterCx!NxNdisPnpPower::ReportNdisMiniportSurpriseRemove+0x1e (Inline Function @ fffff805`3a995962) [minio\netcx\adapter\ndisminiport\km\nxndispnppowerkm.cpp @ 77]

(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : NetAdapterCx!AdapterPnpPower::ReportSurpriseRemoval+0x1e (Inline Function @ fffff805`3a995962) [minio\netcx\adapter\adapterpnppower.cpp @ 538]

fffffd86`c3157780 fffff805`3a9b3318     : ffff9c88`915e001d ffff9c88`6f0a8530 00000000`00000000 fffff805`3a9b399e : NetAdapterCx!AdapterPnpPowerStateMachine<AdapterPnpPower>::EntryFuncs::InterfaceStartedIoStoppedGoingToSurpriseRemovedEntry+0x22 [minio\netcx\adapter\statemachines\AdapterPnpPowerStateMachine.h @ 1060]

(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : NetAdapterCx!SmFx::StateMachineEngine::StateMachineEngineImpl::InvokeStateEntryFunction+0x2c (Inline Function @ fffff805`3a9b3318) [onecore\drivers\smfx\engine\v.current\src\engineimpl.cpp @ 459]

fffffd86`c31577b0 fffff805`3a9b2ed2     : 00000000`00000000 00000000`00000000 ffff9c88`915e4fc8 00000000`00000000 : NetAdapterCx!SmFx::StateMachineEngine::StateMachineEngineImpl::ExecuteCurrentState+0x84 [onecore\drivers\smfx\engine\v.current\src\engineimpl.cpp @ 492]

(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : NetAdapterCx!SmFx::StateMachineEngine::StateMachineEngineImpl::WorkerCallback+0x93 (Inline Function @ fffff805`3a9b2ed2) [onecore\drivers\smfx\engine\v.current\src\engineimpl.cpp @ 1724]

(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : NetAdapterCx!SmFx::StateMachineEngine::StateMachineEngineImpl::Initialize::\_\_l13::<lambda\_c276094d149607b901f7fae525da7e78>::operator()+0x93 (Inline Function @ fffff805`3a9b2ed2) [onecore\drivers\smfx\engine\v.current\src\engineimpl.cpp @ 114]

fffffd86`c3157830 fffff805`3a9b4282     : ffff9c88`94012fa0 ffff9c88`83f3bde0 ffffffff`ffffff00 ffff9c88`94012fa0 : NetAdapterCx!<lambda\_c276094d149607b901f7fae525da7e78>::<lambda\_invoker\_cdecl>+0xa2 [onecore\drivers\smfx\engine\v.current\src\engineimpl.cpp @ 115]

(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : NetAdapterCx!SmFx::Worker::WorkCallback+0xe (Inline Function @ fffff805`3a9b4282) [onecore\drivers\smfx\engine\v.current\src\workerkm.cpp @ 102]

(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : NetAdapterCx!SmFx::Worker::Enqueue::\_\_l2::<lambda\_9395206af589ac42132775cb7e45a067>::operator()+0xe (Inline Function @ fffff805`3a9b4282) [onecore\drivers\smfx\engine\v.current\src\workerkm.cpp @ 93]

fffffd86`c3157860 fffff807`7e0fa8a0     : 00000000`00000000 ffff9c88`94012fa0 00000000`00000000 ffff9c88`83f3bde0 : NetAdapterCx!<lambda\_9395206af589ac42132775cb7e45a067>::<lambda\_invoker\_cdecl>+0x12 [onecore\drivers\smfx\engine\v.current\src\workerkm.cpp @ 94]

fffffd86`c3157890 fffff807`7e016f95     : ffff9c88`6f136c50 ffff9c88`8e632040 fffffd86`c3157a00 ffff9c88`00000000 : nt!IopProcessWorkItem+0x100

fffffd86`c3157900 fffff807`7e10a8b7     : ffff9c88`8e632040 00000000`00000281 ffff9c88`8e632040 fffff807`7e016e40 : nt!ExpWorkerThread+0x155

fffffd86`c3157af0 fffff807`7e22f324     : fffff807`7c3f1180 ffff9c88`8e632040 fffff807`7e10a860 000006ea`0100007f : nt!PspSystemThreadStartup+0x57

fffffd86`c3157b40 00000000`00000000     : fffffd86`c3158000 fffffd86`c3151000 00000000`00000000 00000000`00000000 : nt!KiStartSystemThread+0x34

Looks like a dead lock. Need to continue the debug from OS side.

<https://hsdes.intel.com/appstore/article/#/16018805844>

[USB4V2][BR-POC][RPL-S] BSOD: System Thread Exception\_Not\_Handled | Failure Bucket id:Av\_pci !pci ReservedUSB4powerdependency plug unplug in S0 with TR based docks:

This is Bugcheck 7E - SYSTEM\_THREAD\_EXCEPTION\_NOT\_HANDLED (7e)

8: kd> !analyze -show

SYSTEM\_THREAD\_EXCEPTION\_NOT\_HANDLED (7e)

This is a very common BugCheck.  Usually the exception address pinpoints

the driver/function that caused the problem.  Always note this address

as well as the link date of the driver/image that contains this address.

Arguments:

Arg1: ffffffffc0000005, The exception code that was not handled

Arg2: fffff8065e062adc, The address that the exception occurred at

Arg3: fffff00d3c4b6c08, Exception Record Address

Arg4: fffff00d3c4b6420, Context Record Address

8: kd> u fffff8065e062adc L1

nt!PipCheckValidNewDependencyEdge+0xe4460:

fffff806`5e062adc 488b4910        mov     rcx,qword ptr [rcx+10h]

PCI bus driver tries to add USB4 Power Dependency:

8: kd> k

 # Child-SP          RetAddr               Call Site

00 fffff00d`3c4b5ba8 fffff806`5db8a1f3     nt!KeBugCheckEx

01 (Inline Function) --------`--------     nt!PspUnhandledExceptionInSystemThread+0x33

02 fffff00d`3c4b5bb0 fffff806`5db29f11     nt!PspSystemThreadStartup$filt$0+0x44

03 fffff00d`3c4b5bf0 fffff806`5db757bf     nt!\_\_C\_specific\_handler+0xa1

04 fffff00d`3c4b5c60 fffff806`5d9c7d80     nt!RtlpExecuteHandlerForException+0xf

05 fffff00d`3c4b5c90 fffff806`5d9c733e     nt!RtlDispatchException+0x2c0

06 fffff00d`3c4b63f0 fffff806`5db7f0c5     nt!KiDispatchException+0x1ae

07 fffff00d`3c4b6ad0 fffff806`5db7ae38     nt!KiExceptionDispatch+0x145

08 fffff00d`3c4b6cb0 fffff806`5e062adc     nt!KiPageFault+0x438

09 (Inline Function) --------`--------     nt!RtlFailFast+0x7

0a (Inline Function) --------`--------     nt!FatalListEntryError+0x7

0b (Inline Function) --------`--------     nt!InsertTailList+0xe450f

0c fffff00d`3c4b6e40 fffff806`5db06f20     nt!PipCheckValidNewDependencyEdge+0xe4460

0d fffff00d`3c4b6e70 fffff806`5df7e1fa     nt!PipAddDependencyEdgeBetweenNodes+0x58

0e fffff00d`3c4b6ea0 fffff806`5df7e189     nt!PipSetDependency+0x46

0f fffff00d`3c4b6ed0 fffff806`5ecffdab     nt!IoReserveDependency+0x69

10 fffff00d`3c4b6f30 fffff806`5ecfed42     pci!PciReserveUsb4PowerDependency+0x13b

11 fffff00d`3c4b6fb0 fffff806`5ece3056     pci!PciConstructUsb4PowerDependency+0xa2

12 fffff00d`3c4b7000 fffff806`5ec918c7     pci!PciDevice\_DeviceEnumerated+0x356

13 fffff00d`3c4b7110 fffff806`5dae2369     pci!PciDispatchPnpPower+0x1e7

14 fffff00d`3c4b7180 fffff806`5e1e6492     nt!IopfCallDriver+0x55

15 fffff00d`3c4b71c0 fffff806`5d9978b5     nt!IovCallDriver+0x232

16 fffff00d`3c4b7200 fffff806`5ec2fe24     nt!IofCallDriver+0x85

17 fffff00d`3c4b7240 fffff806`5ec324f3     ACPI!ACPIIrpSetPagableCompletionRoutineAndForward+0x12c

18 fffff00d`3c4b7270 fffff806`5ebb126c     ACPI!ACPIBusIrpDeviceEnumerated+0x313

19 fffff00d`3c4b7310 fffff806`5dae2369     ACPI!ACPIDispatchIrp+0x25c

1a fffff00d`3c4b7390 fffff806`5e1e6492     nt!IopfCallDriver+0x55

1b fffff00d`3c4b73d0 fffff806`5d9978b5     nt!IovCallDriver+0x232

1c fffff00d`3c4b7410 fffff806`5de4d020     nt!IofCallDriver+0x85

1d fffff00d`3c4b7450 fffff806`5daa971b     nt!IopSynchronousCall+0xf8

1e fffff00d`3c4b74c0 fffff806`5de3f61b     nt!PnpIrpDeviceEnumerated+0x3f

1f fffff00d`3c4b7550 fffff806`5df2cff2     nt!PiProcessNewDeviceNode+0xa83

20 fffff00d`3c4b7730 fffff806`5de6eeb7     nt!PiProcessNewDeviceNodeAsync+0x42

21 fffff00d`3c4b7760 fffff806`5deb5e48     nt!PipProcessDevNodeTree+0x3f7

22 fffff00d`3c4b7820 fffff806`5da3e18d     nt!PiProcessReenumeration+0x88

23 fffff00d`3c4b7870 fffff806`5da20765     nt!PnpDeviceActionWorker+0x34d

24 fffff00d`3c4b7940 fffff806`5da980d7     nt!ExpWorkerThread+0x155

25 fffff00d`3c4b7b30 fffff806`5db6dc24     nt!PspSystemThreadStartup+0x57

26 fffff00d`3c4b7b80 00000000`00000000     nt!KiStartSystemThread+0x34

8: kd> .frame /r c

0c fffff00d`3c4b6e40 fffff806`5db06f20     nt!PipCheckValidNewDependencyEdge+0xe4460

rax=ffffcc063ba36d68 rbx=0000000000000000 rcx=0000000000000000

rdx=ffffcc06302f13c0 rsi=fffff00d3c4b6f00 rdi=ffffcc0650564920

rip=fffff8065e062adc rsp=fffff00d3c4b6e40 rbp=fffff00d3c4b6fa0

 r8=ffffcc06328f6790  r9=ffff9687848bc566 r10=ffffcc0650564920

r11=ffffcc06302f13c0 r12=fffff8065ece2d00 r13=0000000000000002

r14=fffff8065eccd000 r15=ffffcc063488f920

iopl=0         nv up ei ng nz na pe nc

cs=0010  ss=0018  ds=002b  es=002b  fs=0053  gs=002b             efl=00040282

nt!PipCheckValidNewDependencyEdge+0xe4460:

fffff806`5e062adc 488b4910        mov     rcx,qword ptr [rcx+10h] ds:002b:00000000`00000010=????????????????

But USB4 device is being removed and its Parent is NULL:

8: kd> dt Provider

Local var @ rdx Type \_PNP\_DEPENDENCY\_NODE\*

   +0x000 ListEntry        : \_LIST\_ENTRY [ 0xffffcc06`3dad0700 - 0xffffcc06`50560a20 ]

   +0x010 Providers        : \_LIST\_ENTRY [ 0xffffcc06`302f13d0 - 0xffffcc06`302f13d0 ]

   +0x020 Dependents       : \_LIST\_ENTRY [ 0xffffcc06`43bc93b0 - 0xffffcc06`43bc89f0 ]

   +0x030 DeviceObject     : 0xffffcc06`3ba36bf0 \_DEVICE\_OBJECT

   +0x038 BindingIds       : \_LIST\_ENTRY [ 0xffff9687`61fca770 - 0xffff9687`61fca770 ]

   +0x048 QueueListEntry   : \_LIST\_ENTRY [ 0xffffcc06`302f1408 - 0xffffcc06`302f1408 ]

   +0x058 ReferenceCount   : 4

   +0x05c Flags            : 0

8: kd> !devstack  0xffffcc06`3ba36bf0

  !DevObj           !DrvObj            !DevExt           ObjectName

> ffffcc063ba36bf0  \Driver\Usb4HostRouterffffcc0644d22f40  000000e7

!DevNode ffffcc0652c3abf0 :

  DeviceInst is "USB4\VIRTUAL\_POWER\_PDO\7&37d92da8&0&0"

8: kd> !DevNode ffffcc0652c3abf0

DevNode 0xffffcc0652c3abf0 for PDO 0xffffcc063ba36bf0

  Parent 0000000000   Sibling 0000000000   Child 0000000000

  InstancePath is "USB4\VIRTUAL\_POWER\_PDO\7&37d92da8&0&0"

  State = DeviceNodeDeletePendingCloses (0x315) @ 2022 Nov 14 07:05:17.470

  Previous State = DeviceNodeAwaitingQueuedDeletion (0x310) @ 2022 Nov 14 07:05:17.000

  StateHistory[00] = DeviceNodeAwaitingQueuedDeletion (0x310)

  StateHistory[19] = DeviceNodeRemovePendingCloses (0x313)

  StateHistory[18] = DeviceNodeStarted (0x30a)

…

The nt!PipCheckValidNewDependencyEdge tries to check if Dependent device is an ancestor of the Provider device, so it attempts to walk Provider’s parent list to IopRootDeviceNode. Since Provider is being removed in this case, the Parent is NULL and this results in nt!PipCheckValidNewDependencyEdge  attempting to dereference a NULL-pointer. The USB4 device failed to own hardware:

8: kd> !wdfdevice 0x000033f9bb2dd3a8 ff

Treating handle as a KMDF handle!

Dumping WDFDEVICE 0x000033f9bb2dd3a8

=================================

WDM PDEVICE\_OBJECTs:  self ffffcc063ba36bf0

Pnp state:  12e ( WdfDevStatePnpFailedWaitForRemove )

…

Pnp state history:

[0] WdfDevStatePnpEnableInterfaces (0x109)

[1] WdfDevStatePnpStarted (0x119)

[2] WdfDevStatePnpSurpriseRemoveIoStarted (0x127)

[3] WdfDevStatePnpFailedIoStarting (0x129)

[4] WdfDevStatePnpFailedOwnHardware (0x12a)

[5] WdfDevStatePnpFailed (0x12b)

[6] WdfDevStatePnpFailedPowerPolicyRemoved (0x139)

[7] WdfDevStatePnpFailedWaitForRemove (0x12e)

…

Regardless of the USB4 HW issues, this seems to be a race condition between USB4 removal and IRP\_MN\_DEVICE\_ENUMERATED/adding power dependency.

<https://hsdes.intel.com/appstore/article/#/16018739951>

“A new guard page for the stack cannot be created.” exception occurs On SparkSpring device:

 Intel WwanConfigurator driver passes destination buffer to memcopy that is too small:

**0:011> !analyze -v**

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**\*                                                                             \***

**\*                        Exception Analysis                                   \***

**\*                                                                             \***

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**APPLICATION\_VERIFIER\_HEAPS\_FIRST\_CHANCE\_ACCESS\_VIOLATION (13)**

**First chance access violation for current stack trace.**

**…**

**CONTEXT:  0000000c4c0fec40 -- (.cxr 0xc4c0fec40)**

**rax=00007ffa7f1b3da0 rbx=0000000000000070 rcx=00007ffa7f1b3da0**

**rdx=000001bca8562fc0 rsi=00007ffa7f1b3da0 rdi=000001bca8562fc0**

**rip=00007ffa7f11c310 rsp=0000000c4c0ff348 rbp=000001bca8562fc0**

**r8=0000000000000070  r9=000001bca8563030 r10=00007ffa7f040000**

**r11=0000000000000246 r12=0000000000000002 r13=00007ffa7f1b7b80**

**r14=0000000000000070 r15=000001bca855cfb0**

**iopl=0         nv up ei ng nz na pe cy**

**cs=0033  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00010283**

**WwanConfigurator!memcpy+0x190:**

**00007ffa`7f11c310 c4a17e6f6c02e0  vmovdqu ymm5,ymmword ptr [rdx+r8-20h] ds:000001bc`a8563010=??**

**Resetting default scope**

**…**

**0:011> k**

**# Child-SP          RetAddr               Call Site**

**00 0000000c`4c0fd6e8 00007ffa`de637cb8     ntdll!ZwWaitForMultipleObjects+0x14**

**01 0000000c`4c0fd6f0 00007ffa`de63728e     ntdll!WerpWaitForCrashReporting+0xa8**

**02 0000000c`4c0fd770 00007ffa`de636a2b     ntdll!RtlReportExceptionHelper+0x33e**

**03 0000000c`4c0fd840 00007ffa`d9592cec     ntdll!RtlReportException+0x9b**

**04 0000000c`4c0fd8c0 00007ffa`de5c7afa     vfbasics!AVrfpVectoredExceptionHandler+0x10c**

**05 0000000c`4c0fd910 00007ffa`de56e882     ntdll!RtlpCallVectoredHandlers+0x112**

**06 (Inline Function) --------`--------     ntdll!RtlCallVectoredExceptionHandlers+0xe**

**07 0000000c`4c0fd9b0 00007ffa`de5f2d5e     ntdll!RtlDispatchException+0x62**

**08 0000000c`4c0fdc00 00007ffa`d96126ee     ntdll!KiUserExceptionDispatch+0x2e**

**09 0000000c`4c0fe300 00007ffa`d961868d     vrfcore!VerifierStopMessageEx+0x81e**

**0a 0000000c`4c0fe660 00007ffa`d97b7383     vrfcore!VfCoreRedirectedStopMessage+0x8d**

**0b 0000000c`4c0fe6f0 00007ffa`de6361af     verifier!VerifierStopMessage+0xc3**

**0c 0000000c`4c0fe7a0 00007ffa`d9592853     ntdll!RtlApplicationVerifierStop+0xef**

**0d 0000000c`4c0fe810 00007ffa`d95936a0     vfbasics!VerifierStopMessage+0x223**

**0e 0000000c`4c0fe870 00007ffa`d9592bfa     vfbasics!AVrfpCheckFirstChanceException+0x148**

**0f 0000000c`4c0fe900 00007ffa`de5c7afa     vfbasics!AVrfpVectoredExceptionHandler+0x1a**

**10 0000000c`4c0fe950 00007ffa`de56e882     ntdll!RtlpCallVectoredHandlers+0x112**

**11 (Inline Function) --------`--------     ntdll!RtlCallVectoredExceptionHandlers+0xe**

**12 0000000c`4c0fe9f0 00007ffa`de5f2d5e     ntdll!RtlDispatchException+0x62**

**13 0000000c`4c0fec40 00007ffa`7f11c310     ntdll!KiUserExceptionDispatch+0x2e**

**14 0000000c`4c0ff348 00007ffa`7f090904     WwanConfigurator!memcpy+0x190**

**15 (Inline Function) --------`--------     WwanConfigurator!memcpy\_s+0x100**

**16 0000000c`4c0ff350 00007ffa`7f09ea9d     WwanConfigurator!mem\_copy+0x144**

**17 0000000c`4c0ff3f0 00007ffa`7f0832a5     WwanConfigurator!Mbim\_memcpy+0x10d**

**18 0000000c`4c0ff470 00007ffa`7f082ea9     WwanConfigurator!ril\_request\_INTC\_THERMAL\_SENSOR\_STATE\_handler+0x1f5**

**19 0000000c`4c0ff940 00007ffa`7f07fc15     WwanConfigurator!on\_request\_thermal\_handler+0x299**

**1a 0000000c`4c0ffa00 00007ffa`dc099363     WwanConfigurator!thermal\_handler+0x475**

**1b 0000000c`4c0ffae0 00007ffa`d95a786e     ucrtbase!thread\_start<unsigned int (\_\_cdecl\*)(void \*),1>+0x93**

**1c 0000000c`4c0ffb10 00007ffa`dd65244d     vfbasics!AVrfpStandardThreadFunction+0x4e**

**1d 0000000c`4c0ffb50 00007ffa`de5adf88     kernel32!BaseThreadInitThunk+0x1d**

**1e 0000000c`4c0ffb80 00000000`00000000     ntdll!RtlUserThreadStart+0x28**

**0:011> .frame /r 18**

**18 0000000c`4c0ff470 00007ffa`7f082ea9     WwanConfigurator!ril\_request\_INTC\_THERMAL\_SENSOR\_STATE\_handler+0x1f5**

**rax=3200000c4c0ff068 rbx=ffffffffffffffff rcx=00007ffade6dce20**

**rdx=0000000c4c0ff6f0 rsi=00007ffa7f13ece0 rdi=000001bca8562fc0**

**rip=00007ffa7f0832a5 rsp=0000000c4c0ff470 rbp=0000000c4c0ff570**

**r8=0000000000000001  r9=0000000c4c0ff1f0 r10=00000001de5adf00**

**r11=0000000c4c0ffb70 r12=0000000000000002 r13=00007ffa7f1b7b80**

**r14=0000000000000000 r15=000001bca855cfb0**

**iopl=0         nv up ei pl zr na po nc**

**cs=0033  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00000246**

**WwanConfigurator!ril\_request\_INTC\_THERMAL\_SENSOR\_STATE\_handler+0x1f5:**

**00007ffa`7f0832a5 41b91c000000    mov     r9d,1Ch**

**0:011> ub**

**WwanConfigurator!ril\_request\_INTC\_THERMAL\_SENSOR\_STATE\_handler+0x1d2:**

**00007ffa`7f083282 418bd1          mov     edx,r9d**

**00007ffa`7f083285 4533c0          xor     r8d,r8d**

**00007ffa`7f083288 e8a3b40100      call    WwanConfigurator!Mbim\_memset (00007ffa`7f09e730)**

**00007ffa`7f08328d 41b970000000    mov     r9d,70h**

**00007ffa`7f083293 488d0d060b1300  lea     rcx,[WwanConfigurator!set\_config (00007ffa`7f1b3da0)]**

**00007ffa`7f08329a 418bd1          mov     edx,r9d**

**00007ffa`7f08329d 4c8bc7          mov     r8,rdi**

**00007ffa`7f0832a0 e8ebb60100      call    WwanConfigurator!Mbim\_memcpy (00007ffa`7f09e990)**

**0:011> db 000001bca8562fc0 L70**

**000001bc`a8562fc0  01 00 00 00 64 00 00 00-01 00 00 00 b0 fa ff ff  ....d...........**

**000001bc`a8562fd0  14 00 00 00 e8 03 00 00-01 00 00 00 01 00 00 00  ................**

**000001bc`a8562fe0  64 00 00 00 02 00 00 00-ff ff ff ff 14 00 00 00  d...............**

**000001bc`a8562ff0  e8 03 00 00 00 00 00 00-d0 d0 d0 d0 d0 d0 d0 d0  ................**

**000001bc`a8563000  ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??  ????????????????**

**000001bc`a8563010  ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??  ????????????????**

**000001bc`a8563020  ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??  ????????????????**

**0:011> lmvi mWwanConfigurator**

**Browse full module list**

**start             end                 module name**

**00007ffa`7f040000 00007ffa`7f1de000   WwanConfigurator   (private pdb symbols)  WwanConfigurator.dll**

**Symbol file: d:\symcache\WwanConfigurator.pdb\C97089E1BCAC48008D8E450174DF4C422\WwanConfigurator.pdb**

**Image path: C:\Windows\System32\WwanConfigurator.dll**

**Image name: WwanConfigurator.dll**

**Browse all global symbols  functions  data**

**Timestamp:        Sat Oct  1 14:02:44 2022 (6338AAF4)**

**CheckSum:         00170672**

**ImageSize:        0019E000**

**File version:     0.6.200.274**

**Product version:  0.6.0.0**

**File flags:       8 (Mask 3F) Private**

**File OS:          40004 NT Win32**

**File type:        3.6 Driver**

**File date:        00000000.00000000**

**Translations:     0409.04b0**

**Information from resource tables:**

**CompanyName:      Intel(R) Corporation**

**ProductName:      Intel(R) Wwan 5G NetAdapter Stack**

**InternalName:     Intel(R) WwanConfigurator Driver"**

**OriginalFilename: WwanConfigurator.dll**

**ProductVersion:   0.6.200.274**

**FileVersion:      0.6.200.274**

**FileDescription:  Intel(R) WwanConfigurator Driver"**

**LegalCopyright:   Copyright(C), 2021 Intel Corporation. All rights reserved.**

<https://hsdes.intel.com/appstore/article/#/16018686259>

[CSPV][CSPV\_SH][ADL][21H2][WOS][LKD]- LKD\_0x17C\_pdc!PdcpLockWatchdogWorkerRoutine:

This is PDC\_LOCK\_WATCHDOG\_LIVEDUMP (17c)

0: kd> !analyze -show

PDC\_LOCK\_WATCHDOG\_LIVEDUMP (17c)

A thread has been holding the PDC lock for too long

(This code can never be used for a real BugCheck.)

Arguments:

Arg1: ffffbb06c8ef1040, The thread holding the PDC lock.

Arg2: 0000000000007530, Lock watchdog timeout in milliseconds.

Arg3: 0000000000000000, Reserved.

Arg4: 0000000000000000, Reserved.

The thread that owns PDC lock for too long is waiting for the Monitor OFF:

0: kd> .thread /p /r ffffbb06c8ef1040

Implicit thread is now ffffbb06`c8ef1040

…

0: kd> k

  \*\*\* Stack trace for last set context - .thread/.cxr resets it

 # Child-SP          RetAddr               Call Site

00 ffffcc0d`e9877290 fffff801`3c06feb7     nt!KiSwapContext+0x76

01 ffffcc0d`e98773d0 fffff801`3c071d69     nt!KiSwapThread+0x3a7

02 ffffcc0d`e98774b0 fffff801`3c075a26     nt!KiCommitThreadWait+0x159

03 ffffcc0d`e9877550 fffff801`3c6dcabe     nt!KeDelayExecutionThread+0x416

04 ffffcc0d`e98775e0 fffff801`3c5f065d     nt!PoBlockConsoleSwitch+0xec3c2

05 ffffcc0d`e9877610 fffff801`4061c28f     nt!PopBlockSessionSwitch+0x3d

06 ffffcc0d`e9877670 fffff801`4062118b     pdc!PdcMonitorControl+0x27

07 ffffcc0d`e98776a0 fffff801`40602b3a     pdc!PdcpTriggerSpecificAction+0xcb

08 ffffcc0d`e9877720 fffff801`406209d2     pdc!PdcpTriggerActionByCaps+0x29e

09 ffffcc0d`e9877820 fffff801`40620308     pdc!PdcpHandleSwitch+0x2ae

0a ffffcc0d`e98778a0 fffff801`406213db     pdc!PdcSystemButtonHandler+0xd8

0b ffffcc0d`e98778e0 fffff801`40602e41     pdc!PdcpPolicyWorkerMain+0x2b

0c ffffcc0d`e9877910 fffff801`3c08ef2f     pdc!PdcpPolicyWorkerThread+0x81

0d ffffcc0d`e9877940 fffff801`3c153175     nt!ExpWorkerThread+0x14f

0e ffffcc0d`e9877b30 fffff801`3c21ed24     nt!PspSystemThreadStartup+0x55

0f ffffcc0d`e9877b80 00000000`00000000     nt!KiStartSystemThread+0x34

0: kd> .frame /r 6

06 ffffcc0d`e9877670 fffff801`4062118b     pdc!PdcMonitorControl+0x27

rax=0000000000000000 rbx=0000000000000000 rcx=0000000000000000

rdx=0000000000000000 rsi=0000000000000004 rdi=000000000000000f

rip=fffff8014061c28f rsp=ffffcc0de9877670 rbp=ffffcc0de9877700

 r8=0000000000000000  r9=0000000000000000 r10=0000000000000000

r11=0000000000000000 r12=0000000000000001 r13=0000000000000000

r14=ffffbb06c2efe8e0 r15=0000000000000000

iopl=0         nv up di pl nz na pe nc

cs=0000  ss=0000  ds=0000  es=0000  fs=0000  gs=0000             efl=00000000

pdc!PdcMonitorControl+0x27:

fffff801`4061c28f 488b055238ffff  mov     rax,qword ptr [pdc!PdcPoCallbacks+0x48 (fffff801`4060fae8)] ds:fffff801`4060fae8={nt!PopControlMonitor (fffff801`3c794160)}

0: kd> dv /V

@ebx              @ebx                         Type = MonitorRequestTypeOff (0n0)

@edi              @edi                RequestReason = MonitorRequestReasonLid (0n15)

ffffcc0d`e98776b0 @rsp+0x0040               Request = struct \_WIN32\_POWERINFO\_MONITOR

ffffcc0d`e98776a0 @rsp+0x0030             SessionId = 0xffffffff

<unavailable>     <unavailable>              Status = <value unavailable>

The System is going through Shutdown however and OS PM worker thread is waiting for the PnP Engine lock:

0: kd> !poaction

…

  Worker thread..: ffffbb06e8ae9080

…

0: kd> .thread /p /r ffffbb06e8ae9080

Implicit thread is now ffffbb06`e8ae9080

…

0: kd> kn

  \*\*\* Stack trace for last set context - .thread/.cxr resets it

 # Child-SP          RetAddr               Call Site

00 ffffcc0d`e9d3ec90 fffff801`3c06feb7     nt!KiSwapContext+0x76

01 ffffcc0d`e9d3edd0 fffff801`3c071d69     nt!KiSwapThread+0x3a7

02 ffffcc0d`e9d3eeb0 fffff801`3c06bc84     nt!KiCommitThreadWait+0x159

03 ffffcc0d`e9d3ef50 fffff801`3c13187d     nt!KeWaitForSingleObject+0x234

04 ffffcc0d`e9d3f040 fffff801`3c06aea6     nt!ExpWaitForResource+0x6d

05 ffffcc0d`e9d3f0c0 fffff801`3c4f0d35     nt!ExAcquireResourceExclusiveLite+0x196

06 ffffcc0d`e9d3f150 fffff801`3c1562cc     nt!PpDevNodeLockTree+0x59

07 ffffcc0d`e9d3f180 fffff801`3c84d736     nt!PnpLockDeviceActionQueue+0x18

08 ffffcc0d`e9d3f1c0 fffff801`3c84d6aa     nt!IoBuildPoDeviceNotifyList+0x4a

09 ffffcc0d`e9d3f220 fffff801`3c5f461e     nt!PopBuildDeviceNotifyList+0xba

0a ffffcc0d`e9d3f300 fffff801`3c84613d     nt!PoInitializeBroadcast+0xbe

0b ffffcc0d`e9d3f330 fffff801`3c84fa0c     nt!PopTransitionSystemPowerStateEx+0x235

0c ffffcc0d`e9d3f3f0 fffff801`3c22d275     nt!NtSetSystemPowerState+0x4c

0d ffffcc0d`e9d3f5c0 fffff801`3c21f4c0     nt!KiSystemServiceCopyEnd+0x25

0e ffffcc0d`e9d3f758 fffff801`3c84604b     nt!KiServiceLinkage

0f ffffcc0d`e9d3f760 fffff801`3c84fa0c     nt!PopTransitionSystemPowerStateEx+0x143

10 ffffcc0d`e9d3f820 fffff801`3c4354c4     nt!NtSetSystemPowerState+0x4c

11 ffffcc0d`e9d3f9f0 fffff801`3c22d275     nt!NtShutdownSystem+0x74

12 ffffcc0d`e9d3fa20 00007ff8`a9647334     nt!KiSystemServiceCopyEnd+0x25

13 00000026`4687f388 00000000`00000000     0x00007ff8`a9647334

0: kd> .frame /r 6

06 ffffcc0d`e9d3f150 fffff801`3c1562cc     nt!PpDevNodeLockTree+0x59

rax=0000000000000000 rbx=0000000000000001 rcx=0000000000000000

rdx=0000000000000000 rsi=0000000000000000 rdi=ffffffffffffffff

rip=fffff8013c4f0d35 rsp=ffffcc0de9d3f150 rbp=ffffcc0de9d3f200

 r8=0000000000000000  r9=0000000000000000 r10=0000000000000000

r11=0000000000000000 r12=ffffcc0de9d3f4fc r13=ffffcc0de9d3f4f8

r14=0000000000000005 r15=ffffbb075ef56d30

iopl=0         nv up di pl nz na pe nc

cs=0000  ss=0000  ds=0000  es=0000  fs=0000  gs=0000             efl=00000000

nt!PpDevNodeLockTree+0x59:

fffff801`3c4f0d35 ebca            jmp     nt!PpDevNodeLockTree+0x25 (fffff801`3c4f0d01)

0: kd> ub

nt!PpDevNodeLockTree+0x43:

fffff801`3c4f0d1f 5f              pop     rdi

fffff801`3c4f0d20 c3              ret

fffff801`3c4f0d21 cc              int     3

fffff801`3c4f0d22 83e901          sub     ecx,1

fffff801`3c4f0d25 7510            jne     nt!PpDevNodeLockTree+0x5b (fffff801`3c4f0d37)

fffff801`3c4f0d27 8ad3            mov     dl,bl

fffff801`3c4f0d29 488d0d90535500  lea     rcx,[nt!PiEngineLock (fffff801`3ca460c0)]

fffff801`3c4f0d30 e8db9fb7ff      call    nt!ExAcquireResourceExclusiveLite (fffff801`3c06ad10)

The PnP Engine lock is taken by NDIS thread going through device removal and, as it unregisters as PDC client is waiting for the PDC lock:

0: kd> !locks nt!PiEngineLock

Resource @ nt!PiEngineLock (0xfffff8013ca460c0)    Exclusively owned

    Contention Count = 23

    NumberOfExclusiveWaiters = 1

     Threads: ffffbb06b71c7040-01<\*>

     Threads Waiting On Exclusive Access:

              ffffbb06e8ae9080

1 total locks

0: kd> .thread /p /r ffffbb06b71c7040

Implicit thread is now ffffbb06`b71c7040

…

0: kd> kn

  \*\*\* Stack trace for last set context - .thread/.cxr resets it

 # Child-SP          RetAddr               Call Site

00 ffffcc0d`e8e499e0 fffff801`3c06feb7     nt!KiSwapContext+0x76

01 ffffcc0d`e8e49b20 fffff801`3c071d69     nt!KiSwapThread+0x3a7

02 ffffcc0d`e8e49c00 fffff801`3c06bc84     nt!KiCommitThreadWait+0x159

03 ffffcc0d`e8e49ca0 fffff801`3c13187d     nt!KeWaitForSingleObject+0x234

04 ffffcc0d`e8e49d90 fffff801`3c06aea6     nt!ExpWaitForResource+0x6d

05 ffffcc0d`e8e49e10 fffff801`40619dd6     nt!ExAcquireResourceExclusiveLite+0x196

06 ffffcc0d`e8e49ea0 fffff801`4061bcdd     pdc!PdcAcquireLock+0x36

07 ffffcc0d`e8e49ed0 fffff801`40e48099     pdc!PdcpProcessReceivedKernelMessage+0x1d

08 ffffcc0d`e8e49f00 fffff801`40e47eb1     ndis!PdcpPortReleaseResources+0x5d

09 ffffcc0d`e8e4a250 fffff801`40e47dea     ndis!PdcPortClose+0x35

0a ffffcc0d`e8e4a280 fffff801`40e3a5f1     ndis!PdcTaskClientUnregister+0x3a

0b ffffcc0d`e8e4a2b0 fffff801`40d75965     ndis!ndisMDeRegisterPDCTaskClient+0x61

0c ffffcc0d`e8e4a2f0 fffff801`40e3a0ac     ndis!ndisMDeleteMiniportBlockOnRemove+0x25

0d ffffcc0d`e8e4a320 fffff801`40d51946     ndis!ndisPnPIrpRemoveDevice+0x238

0e ffffcc0d`e8e4a390 fffff801`3c042665     ndis!ndisPnPDispatch+0x179f6

0f ffffcc0d`e8e4a400 fffff801`3c4bfcf4     nt!IofCallDriver+0x55

10 ffffcc0d`e8e4a440 fffff801`3c56cc60     nt!IopSynchronousCall+0xf8

11 ffffcc0d`e8e4a4b0 fffff801`3c10bf45     nt!IopRemoveDevice+0x108

12 ffffcc0d`e8e4a560 fffff801`3c56c7a2     nt!PnpRemoveLockedDeviceNode+0x1a9

13 ffffcc0d`e8e4a5c0 fffff801`3c56c507     nt!PnpDeleteLockedDeviceNode+0x52

14 ffffcc0d`e8e4a600 fffff801`3c600d31     nt!PnpDeleteLockedDeviceNodes+0xcf

15 ffffcc0d`e8e4a680 fffff801`3c600c59     nt!PipRemoveDevicesInRelationList+0x8d

16 ffffcc0d`e8e4a6d0 fffff801`3c600aa4     nt!PnpDelayedRemoveWorker+0x119

17 ffffcc0d`e8e4a720 fffff801`3c1a3805     nt!PnpChainDereferenceComplete+0xf4

18 ffffcc0d`e8e4a750 fffff801`3c56afa9     nt!PnpIsChainDereferenced+0xad

19 ffffcc0d`e8e4a7b0 fffff801`3c4c3261     nt!PnpProcessQueryRemoveAndEject+0x2a5

1a ffffcc0d`e8e4a890 fffff801`3c4c72d5     nt!PnpProcessTargetDeviceEvent+0x109

1b ffffcc0d`e8e4a8c0 fffff801`3c08ef2f     nt!PnpDeviceEventWorker+0x2c5

1c ffffcc0d`e8e4a940 fffff801`3c153175     nt!ExpWorkerThread+0x14f

1d ffffcc0d`e8e4ab30 fffff801`3c21ed24     nt!PspSystemThreadStartup+0x55

1e ffffcc0d`e8e4ab80 00000000`00000000     nt!KiStartSystemThread+0x34

0: kd> .frame /r 6

06 ffffcc0d`e8e49ea0 fffff801`4061bcdd     pdc!PdcAcquireLock+0x36

rax=0000000000000000 rbx=000000004bb9e2cf rcx=0000000000000000

rdx=0000000000000000 rsi=ffffcd07649139f0 rdi=ffffcc0de8e49f20

rip=fffff80140619dd6 rsp=ffffcc0de8e49ea0 rbp=fffff80140de1780

 r8=0000000000000000  r9=0000000000000000 r10=0000000000000000

r11=0000000000000000 r12=ffffcd0777c5a730 r13=fffff80140dfb050

r14=ffffcc0de8e4a410 r15=ffffbb06dcbe5050

iopl=0         nv up di pl nz na pe nc

cs=0000  ss=0000  ds=0000  es=0000  fs=0000  gs=0000             efl=00000000

pdc!PdcAcquireLock+0x36:

fffff801`40619dd6 65488b0c2588010000 mov   rcx,qword ptr gs:[188h] gs:00000000`00000188=????????????????

0: kd> ub

pdc!PdcAcquireLock+0xd:

fffff801`40619dad e80e39a0fb      call    nt!KeEnterCriticalRegion (fffff801`3c01d6c0)

fffff801`40619db2 4c8b15ff85ffff  mov     r10,qword ptr [pdc!\_imp\_KeQueryUnbiasedInterruptTime (fffff801`406123b8)]

fffff801`40619db9 e8e2a1aafb      call    nt!KeQueryUnbiasedInterruptTime (fffff801`3c0c3fa0)

fffff801`40619dbe b201            mov     dl,1

fffff801`40619dc0 488d0d395effff  lea     rcx,[pdc!PdcLock (fffff801`4060fc00)]

fffff801`40619dc7 488bd8          mov     rbx,rax

fffff801`40619dca 4c8b150784ffff  mov     r10,qword ptr [pdc!\_imp\_ExAcquireResourceExclusiveLite (fffff801`406121d8)]

fffff801`40619dd1 e83a0fa5fb      call    nt!ExAcquireResourceExclusiveLite (fffff801`3c06ad10)

The PDC lock, however is taken by the thread waiting for the Monitor OFF:

0: kd> !locks pdc!PdcLock

Resource @ pdc!PdcLock (0xfffff8014060fc00)    Exclusively owned

    Contention Count = 17

    NumberOfExclusiveWaiters = 12

     Threads: ffffbb06c8ef1040-01<\*>

     Threads Waiting On Exclusive Access:

              ffffbb0760af4580       ffffbb06c8df1040       ffffbb076141f040       ffffbb0760e91040

              ffffbb0760a6b080       ffffbb075ee17040       ffffbb075cdb4080       ffffbb0760a2a080

              ffffbb06b71c7040       ffffbb0763a06040       ffffbb0762410040       ffffbb07602e1080

1 total locks

0: kd> !thread ffffbb06c8ef1040

THREAD ffffbb06c8ef1040  Cid 0004.026c  Teb: 0000000000000000 Win32Thread: 0000000000000000 WAIT: (DelayExecution) KernelMode Non-Alertable

    ffffffffffffffff  NotificationEvent

Not impersonating

DeviceMap                 ffffcd075ae33920

Owning Process            ffffbb06b70fd040       Image:         System

Attached Process          N/A            Image:         N/A

Wait Start TickCount      9024           Ticks: 0

Context Switch Count      16445          IdealProcessor: 4  NoStackSwap

UserTime                  00:00:00.000

KernelTime                00:00:00.125

Win32 Start Address nt!ExpWorkerThread (0xfffff8013c08ede0)

Stack Init ffffcc0de9877bb0 Current ffffcc0de9877250

Base ffffcc0de9878000 Limit ffffcc0de9871000 Call 0000000000000000

Priority 15 BasePriority 12 PriorityDecrement 48 IoPriority 2 PagePriority 5

Child-SP          RetAddr               : Args to Child                                                           : Call Site

ffffcc0d`e9877290 fffff801`3c06feb7     : ffff8000`00000000 00000000`00000000 00000000`00000000 ffffbb06`c8ef1040 : nt!KiSwapContext+0x76

ffffcc0d`e98773d0 fffff801`3c071d69     : ffffbb06`00000004 00000000`00000000 00000000`00000000 00000000`00000000 : nt!KiSwapThread+0x3a7

ffffcc0d`e98774b0 fffff801`3c075a26     : 00000000`00000000 00000000`00000000 00000000`00000003 00000000`540da55f : nt!KiCommitThreadWait+0x159

ffffcc0d`e9877550 fffff801`3c6dcabe     : 00000000`00000000 fffff801`3c06d3ed ffff8000`c78c0100 00000000`00000002 : nt!KeDelayExecutionThread+0x416

ffffcc0d`e98775e0 fffff801`3c5f065d     : 00000000`ffffffff ffffffff`fffe7960 00000000`00000002 fffff801`3c21f4c0 : nt!PoBlockConsoleSwitch+0xec3c2

ffffcc0d`e9877610 fffff801`4061c28f     : ffffbb06`b70c9c60 ffffbb06`d24e5040 00000000`00000001 00000000`00000000 : nt!PopBlockSessionSwitch+0x3d

ffffcc0d`e9877670 fffff801`4062118b     : 00000000`ffffffff 00000000`00000001 00000000`00000001 ffffcd07`00000000 : pdc!PdcMonitorControl+0x27

ffffcc0d`e98776a0 fffff801`40602b3a     : ffffbb06`b70c9c60 fffff801`3c01daa2 00000000`000a0000 00000000`00000000 : pdc!PdcpTriggerSpecificAction+0xcb

ffffcc0d`e9877720 fffff801`406209d2     : fffff801`00000000 ffffbb06`c2efe8e0 00000000`00000000 00000000`00000000 : pdc!PdcpTriggerActionByCaps+0x29e

ffffcc0d`e9877820 fffff801`40620308     : ffffbb06`c2efe8e0 fffff801`4060e4c0 ffffbb06`c56e8dd0 ffffbb06`c26ffd10 : pdc!PdcpHandleSwitch+0x2ae

ffffcc0d`e98778a0 fffff801`406213db     : 00000000`00000000 00000000`00000000 00000000`00000001 00000000`00000000 : pdc!PdcSystemButtonHandler+0xd8

ffffcc0d`e98778e0 fffff801`40602e41     : ffffbb06`b70c9c60 00000000`80000000 ffffbb06`b70c9c60 ffffbb06`d02e2af0 : pdc!PdcpPolicyWorkerMain+0x2b

ffffcc0d`e9877910 fffff801`3c08ef2f     : ffffbb06`00000000 ffffbb06`c8ef1040 ffffbb06`b70c9c60 00000000`00000000 : pdc!PdcpPolicyWorkerThread+0x81

ffffcc0d`e9877940 fffff801`3c153175     : ffffbb06`c8ef1040 ffff8000`c7ad0000 ffffbb06`c8ef1040 006fe47f`b19bbdff : nt!ExpWorkerThread+0x14f

ffffcc0d`e9877b30 fffff801`3c21ed24     : ffff8000`c7ac0180 ffffbb06`c8ef1040 fffff801`3c153120 00000000`00000000 : nt!PspSystemThreadStartup+0x55

ffffcc0d`e9877b80 00000000`00000000     : ffffcc0d`e9878000 ffffcc0d`e9871000 00000000`00000000 00000000`00000000 : nt!KiStartSystemThread+0x34

So this appears to be OS deadlock leading to the live dump, and, potentially Bugcheck 9F as well.

<https://hsdes.intel.com/appstore/article/#/22016115730>

(WIFI-258183)[WIN11][SV1][NetAdapter] OS doesn't trigger phase 2 for PLDR ending in BSOD 0x9F:

This is Bugcheck 9F - DRIVER\_POWER\_STATE\_FAILURE (9f)

0: kd> !analyze -show

DRIVER\_POWER\_STATE\_FAILURE (9f)

A driver has failed to complete a power IRP within a specific time.

Arguments:

Arg1: 0000000000000003, A device object has been blocking an IRP for too long a time

Arg2: ffffda05131cd570, Physical Device Object of the stack

Arg3: fffff802821dd738, nt!TRIAGE\_9F\_POWER on Win7 and higher, otherwise the Functional Device Object of the stack

Arg4: ffffda05303c2aa0, The blocked IRP

The timed-out power IRP is owned by the Wifi driver:

0: kd> !irp ffffda05303c2aa0

Irp is active with 9 stacks 8 is current (= 0xffffda05303c2d68)

 No Mdl: No System Buffer: Thread 00000000:  Irp stack trace.  Pending has been returned

     cmd  flg cl Device   File     Completion-Context

…

 [IRP\_MJ\_POWER(16), IRP\_MN\_WAIT\_WAKE(0)]

            0  0 ffffda05131cd570 00000000 00000000-00000000

             \Driver\pci

                  Args: 00000000 00000000 00000000 00000002

>[IRP\_MJ\_POWER(16), IRP\_MN\_SET\_POWER(2)]

            0 e1 ffffda0531367de0 00000000 fffff8027e19f290-ffffda055027d4a8 Success Error Cancel pending

             \Driver\Netwaw12 nt!PopRequestCompletion

                  Args: 00051100 00000001 00000001 00000002

 [N/A(0), N/A(0)]

            0  0 00000000 00000000 00000000-ffffda055027d4a8

                  Args: 00000000 00000000 00000000 00000000

0: kd> !devstack ffffda0531367de0

  !DevObj           !DrvObj            !DevExt           ObjectName

> ffffda0531367de0  \Driver\Netwaw12   ffffda052bc20c60

  ffffda051310ed30  \Driver\ACPI       ffffda050aef0260

  ffffda05131cd570  \Driver\pci        ffffda05131cd6c0  NTPNP\_PCI0029

!DevNode ffffda05131ce7e0 :

  DeviceInst is "PCI\VEN\_8086&DEV\_272B&SUBSYS\_00F08086&REV\_1A\4&c921094&0&00E0"

  ServiceName is "Netwaw12"

But KMDF is waiting for the power event processing to start self-managed I/O:

0: kd> !wdfkd.wdfdriverinfo Netwaw12

----------------------------------

Default driver image name: Netwaw12

WDF library image name: Wdf01000

 FxDriverGlobals  0xffffda0531e38dc0

 WdfBindInfo      0xfffff802d0dd76e0

   Version        v1.31

 Library module   0xffffda050c1f1eb0

   ServiceName    \Registry\Machine\System\CurrentControlSet\Services\Wdf01000

   ImageName      Wdf01000

----------------------------------

WDFDRIVER: 0x000025faafc58c98

Driver logs: Not available

Framework logs: !wdflogdump Netwaw12.sys -f

    !wdfdevice 0x000025fad43df688 ff (FDO)

…

0: kd> !wdfdevice 0x000025fad43df688 ff

Treating handle as a KMDF handle!

Dumping WDFDEVICE 0x000025fad43df688

=================================

WDM PDEVICE\_OBJECTs: self 0xFFFFDA0531367DE0 attached 0xFFFFDA051310ED30 pdo 0xFFFFDA05131CD570

Pnp state:  119 ( WdfDevStatePnpStarted )

Power state:  32b ( WdfDevStatePowerStartSelfManagedIo )

Power Pol state:  52f ( WdfDevStatePwrPolSystemWakeDeviceToD0CompletePowerUp )

…

owning thread:  ffffda052cf66040

Power state history:

[0] WdfDevStatePowerDx (0x31f)

[1] WdfDevStatePowerCheckDeviceType (0x301)

[2] WdfDevStatePowerWaking (0x333)

[3] WdfDevStatePowerNotifyingD0EntryToWakeInterrupts (0x35a)

[4] WdfDevStatePowerWakingConnectInterrupt (0x335)

[5] WdfDevStatePowerWakingDmaEnable (0x339)

[6] WdfDevStatePowerWakingPostHardwareEnabled (0x363)

[7] WdfDevStatePowerStartSelfManagedIo (0x32b)

…

0: kd> !thread ffffda052cf66040

THREAD ffffda052cf66040  Cid 0004.03c0  Teb: 0000000000000000 Win32Thread: 0000000000000000 WAIT: (Executive) KernelMode Non-Alertable

    ffffda05388e0cd0  NotificationEvent

Not impersonating

DeviceMap                 ffffb78aff8833b0

Owning Process            ffffda050aaf3040       Image:         System

Attached Process          N/A            Image:         N/A

Wait Start TickCount      39853          Ticks: 7422 (0:00:01:55.968)

Context Switch Count      41075          IdealProcessor: 11  NoStackSwap

UserTime                  00:00:00.000

KernelTime                00:00:00.515

Win32 Start Address nt!ExpWorkerThread (0xfffff8027e0cce40)

Stack Init ffffb4086ff57bb0 Current ffffb4086ff56700

Base ffffb4086ff58000 Limit ffffb4086ff51000 Call 0000000000000000

Priority 14 BasePriority 12 PriorityDecrement 0 IoPriority 2 PagePriority 5

Child-SP          RetAddr               : Args to Child                                                           : Call Site

ffffb408`6ff56740 fffff802`7e08ed85     : 00000000`00000000 00000000`00000000 00000000`0004fade ffff8200`d0dc0180 : nt!KiSwapContext+0x76

ffffb408`6ff56880 fffff802`7e0901a7     : ffffda05`2cf66040 ffffda05`00000000 00000000`00000000 00000000`00000000 : nt!KiSwapThread+0xa65

ffffb408`6ff569d0 fffff802`7e0924c6     : 00000001`00000000 00000000`00000001 00000000`00000000 00000000`00000000 : nt!KiCommitThreadWait+0x137

ffffb408`6ff56a80 fffff802`809d6763     : 00000000`5270784e 00000000`00000103 000025fa`d43df601 00000000`00000000 : nt!KeWaitForSingleObject+0x256

(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : Wdf01000!MxEvent::WaitFor+0x21 (Inline Function @ fffff802`809d6763)

(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : Wdf01000!FxCREvent::EnterCRAndWait+0x2d (Inline Function @ fffff802`809d6763)

(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : Wdf01000!FxCREvent::EnterCRAndWaitAndLeave+0x2d (Inline Function @ fffff802`809d6763)

(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : Wdf01000!FxPowerIdleMachine::WaitForD0+0x2d (Inline Function @ fffff802`809d6763)

ffffb408`6ff56e20 fffff802`809f1629     : 00000000`00000003 00000000`5270784e 00000000`00000001 ffff280f`a3400bb0 : Wdf01000!FxPowerIdleMachine::PowerReferenceWorker+0xddcb

(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : Wdf01000!FxPowerIdleMachine::PowerReference+0x2e (Inline Function @ fffff802`809f1629)

(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : Wdf01000!FxPkgPnp::PowerReference+0x33 (Inline Function @ fffff802`809f1629)

ffffb408`6ff56e90 fffff802`809f38fb     : ffffda05`2bc20970 ffffda05`2ab36f00 00000000`00000001 ffffda05`3e6e8000 : Wdf01000!StopIdleWorker+0xe5

ffffb408`6ff56ee0 fffff802`d1165f8b     : ffffda05`3e6e8fd8 fffff802`7af612d3 fffff802`00000006 ffffb408`6ff56fc0 : Wdf01000!imp\_WdfDeviceStopIdleActual+0x1b

(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : NetAdapterCx!WdfDeviceStopIdleActual+0x35 (Inline Function @ fffff802`d1165f8b)

ffffb408`6ff56f20 fffff802`d113a78e     : ffffda05`3e4ea950 00000000`0000000f 00000000`00000021 fffff802`817bc218 : NetAdapterCx!NxPowerReference::PowerReference+0x97

(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : NetAdapterCx!NxPowerPolicy::PowerReference+0x5 (Inline Function @ fffff802`d113a78e)

(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : NetAdapterCx!NxAdapter::PowerReference+0x5 (Inline Function @ fffff802`d113a78e)

ffffb408`6ff56f70 fffff802`817ee59c     : ffffda05`3e4ea950 00000000`00000000 ffffb408`6ff50021 ffffb408`6ff57018 : NetAdapterCx!EvtNdisPowerReference+0x6e

ffffb408`6ff56fa0 fffff802`8185d955     : ffffda05`3e4ea950 00000000`00000001 ffffda05`3e6e8030 ffffda05`3e6e8030 : ndis!ndisWdfAcquirePowerReferenceHelper+0x30

ffffb408`6ff56ff0 fffff802`81800538     : ffffda05`3e6e8030 00000000`00000000 00000000`00000000 ffffda05`00000027 : ndis!ndisSelectiveSuspendStop+0x25d

ffffb408`6ff57060 fffff802`8182ecb7     : ffffda05`3e6e8030 00000000`00000000 00000000`00000000 00000000`00000000 : ndis!ndisPowerSaveStop+0x384f0

ffffb408`6ff57090 fffff802`8180faad     : 00000000`00000000 fffff802`d12491a0 fffff802`d1171b80 00000000`00000000 : ndis!ndisPnPIrpStopDevice+0x8b

ffffb408`6ff57100 fffff802`d11628ad     : ffffda05`387f3a80 00000000`00000000 00000000`00000001 fffff802`7e0d8b5f : ndis!NdisWdfPnpPowerEventHandler+0xed

ffffb408`6ff57140 fffff802`d1135b01     : ffffda05`4adfb8f0 fffff802`d1154138 00000000`00000009 ffffda05`4adfbcd8 : NetAdapterCx!NxNdisPnpMiniport::StopNdisMiniport+0x1d

(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : NetAdapterCx!AdapterPnpPower::StopNetworkInterface+0x1b (Inline Function @ fffff802`d1135b01)

ffffb408`6ff57170 fffff802`d1153318     : ffffda05`4adfb8f0 00000000`00000000 00000000`00000000 fffff802`d1171b50 : NetAdapterCx!AdapterPnpPowerStateMachine<AdapterPnpPower>::EntryFuncs::StopNetworkInterfaceEntry+0x21

(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : NetAdapterCx!SmFx::StateMachineEngine::StateMachineEngineImpl::InvokeStateEntryFunction+0x2c (Inline Function @ fffff802`d1153318)

ffffb408`6ff571a0 fffff802`d1153b4c     : ffffda05`4adfb8f0 00000000`00000000 00000000`00000009 00000000`00000008 : NetAdapterCx!SmFx::StateMachineEngine::StateMachineEngineImpl::ExecuteCurrentState+0x84

ffffb408`6ff57220 fffff802`d1152ccf     : ffffda05`4adfb8f0 00000000`00000001 00000000`0000000d 00000000`00000000 : NetAdapterCx!SmFx::StateMachineEngine::StateMachineEngineImpl::ProcessEventQueue+0x138

(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : NetAdapterCx!SmFx::StateMachineEngine::StateMachineEngineImpl::EnqueueEvent+0xdd (Inline Function @ fffff802`d1152ccf)

ffffb408`6ff57270 fffff802`d11352b5     : ffffda05`387f3a80 00000000`00000001 000025fa`c79b9c98 00000000`0000002b : NetAdapterCx!SmFx::StateMachineEngine::EnqueueEvent+0xfb

(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : NetAdapterCx!AdapterPnpPowerStateMachine<AdapterPnpPower>::EnqueueEvent+0xd (Inline Function @ fffff802`d11352b5)

ffffb408`6ff572b0 fffff802`d113e8a9     : 000025fa`c79b9c98 ffffb408`6ff57380 00000000`00000004 00000000`00000000 : NetAdapterCx!AdapterPnpPower::NetAdapterStop+0xb9

(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : NetAdapterCx!AdapterPnpPower::NetAdapterStop+0x13 (Inline Function @ fffff802`d113e8a9)

ffffb408`6ff57320 fffff802`d1219617     : 00000000`00000000 000025fa`c79b9c98 ffffda05`30f6c070 ffffda05`30f6c068 : NetAdapterCx!imp\_NetAdapterStop+0x59

ffffb408`6ff57350 fffff802`d121992f     : fffff802`d12491a0 00000000`00000000 00000000`00000000 ffffda05`50359b60 : WifiCx!WxDevice::DeleteInnerPort+0xeb

ffffb408`6ff573c0 fffff802`d1219c92     : 00000000`00000005 ffffda05`30f6c030 00000000`00000003 fffff802`80a54a9c : WifiCx!WxDevice::DeletePortTypes+0x233

ffffb408`6ff57440 fffff802`d1217b65     : 00000000`00000005 00000000`0000000c 00000000`00000001 ffffda05`30f6c030 : WifiCx!WxDevice::PostSelfManagedIoSuspendEx+0xde

ffffb408`6ff574a0 fffff802`80a2d66d     : ffffda05`497668c0 00000000`00000000 00000000`00000004 ffffda05`31e38dc0 : WifiCx!EvtCxDevicePostSelfManagedIoSuspendEx+0x55

ffffb408`6ff574d0 fffff802`80a39ac4     : ffffda05`497668c0 00000000`00000000 ffffb408`6ff5000c ffffb408`6ff575e8 : Wdf01000!FxPnpDeviceSelfManagedIoSuspend::InvokeCxCallback+0x5d

But the worker thread is waiting for the Power Machine state lock:

0: kd> .thread /p /r ffffda0513185040

Implicit thread is now ffffda05`13185040

…

0: kd> !thread  ffffda0513185040

THREAD ffffda0513185040  Cid 0004.01e4  Teb: 0000000000000000 Win32Thread: 0000000000000000 WAIT: (Executive) KernelMode Non-Alertable

    ffffda050cb8aab8  SynchronizationEvent

Not impersonating

DeviceMap                 ffffb78aff8833b0

Owning Process            ffffda050aaf3040       Image:         System

Attached Process          N/A            Image:         N/A

Wait Start TickCount      39622          Ticks: 7653 (0:00:01:59.578)

Context Switch Count      406            IdealProcessor: 0  NoStackSwap

UserTime                  00:00:00.000

KernelTime                00:00:00.046

Win32 Start Address nt!ExpWorkerThread (0xfffff8027e0cce40)

Stack Init ffffb4086f305bb0 Current ffffb4086f3050c0

Base ffffb4086f306000 Limit ffffb4086f2ff000 Call 0000000000000000

Priority 15 BasePriority 12 PriorityDecrement 0 IoPriority 2 PagePriority 5

Child-SP          RetAddr               : Args to Child                                                           : Call Site

ffffb408`6f305100 fffff802`7e08ed85     : 00000000`00000000 00000000`00000000 00000000`000021ae ffff8200`d0821180 : nt!KiSwapContext+0x76

ffffb408`6f305240 fffff802`7e0901a7     : ffffda05`13185040 ffffda05`00000000 00000000`00000000 00000000`00000000 : nt!KiSwapThread+0xa65

ffffb408`6f305390 fffff802`7e0924c6     : ffffda05`00000000 00000000`00000001 ffff0000`00000000 00000000`00000000 : nt!KiCommitThreadWait+0x137

ffffb408`6f305440 fffff802`809c13a2     : ffffda05`2cf66040 00000000`00000000 ffffda05`2cf66040 00000000`00000000 : nt!KeWaitForSingleObject+0x256

(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : Wdf01000!MxEvent::WaitFor+0x2a (Inline Function @ fffff802`809c13a2)

ffffb408`6f3057e0 fffff802`80a30917     : ffffb408`6f305870 00000000`00000000 00000000`00000000 ffffda05`13185040 : Wdf01000!FxWaitLockInternal::AcquireLock+0x56

ffffb408`6f305820 fffff802`80a41271     : ffffda05`0cb8aab0 ffffda05`0cb8aa90 00000000`00000000 fffff802`7e0ceb33 : Wdf01000!FxPkgPnp::\_PowerProcessEventInner+0x27

ffffb408`6f305850 fffff802`80a4157c     : ffffda05`31906270 ffffda05`31367de0 00000000`00000000 00000000`00000100 : Wdf01000!FxEventQueue::EventQueueWorker+0x75

ffffb408`6f3058a0 fffff802`7e0beba0     : ffffda05`00000000 ffffda05`31906270 00000000`00000000 ffffda05`31367de0 : Wdf01000!FxThreadedEventQueue::\_WorkItemCallback+0xc

ffffb408`6f3058d0 fffff802`7e0ccf95     : ffffda05`0ab5cbb0 ffffda05`13185040 ffffda05`31906270 00000000`00000000 : nt!IopProcessWorkItem+0x100

ffffb408`6f305940 fffff802`7e0c4807     : ffffda05`13185040 ffff8200`d11e0000 ffffda05`13185040 006fe47f`b19bbdff : nt!ExpWorkerThread+0x155

ffffb408`6f305b30 fffff802`7e2250d4     : ffff8200`d11d1180 ffffda05`13185040 fffff802`7e0c47b0 00000000`00000000 : nt!PspSystemThreadStartup+0x57

ffffb408`6f305b80 00000000`00000000     : ffffb408`6f306000 ffffb408`6f2ff000 00000000`00000000 00000000`00000000 : nt!KiStartSystemThread+0x34

The Power Machine state lock however is owned by the power thread:

0: kd> .frame /r 5

05 ffffb408`6f3057e0 fffff802`80a30917     Wdf01000!FxWaitLockInternal::AcquireLock+0x56

rax=0000000000000000 rbx=0000000000000000 rcx=0000000000000000

rdx=0000000000000000 rsi=ffffda050cb8aab8 rdi=ffffda050cb8aab8

rip=fffff802809c13a2 rsp=ffffb4086f3057e0 rbp=0000000000000000

 r8=0000000000000000  r9=0000000000000000 r10=0000000000000000

r11=0000000000000000 r12=0000000000000100 r13=0000000000000000

r14=fffff80280a41570 r15=ffffda0531906270

iopl=0         nv up di pl nz na pe nc

cs=0000  ss=0000  ds=0000  es=0000  fs=0000  gs=0000             efl=00000000

Wdf01000!FxWaitLockInternal::AcquireLock+0x56:

fffff802`809c13a2 8bd8            mov     ebx,eax

0: kd> dt this

Local var @ rdi Type FxWaitLockInternal\*

   +0x000 m\_Event          : MxEvent

   +0x020 m\_OwningThread   : 0xffffda05`2cf66040 \_KTHREAD

So this appears to be a deadlock leading to the power IRP timeout.

<https://hsdes.intel.com/appstore/article/#/16018645471>

“A new guard page for the stack cannot be created.” exception occurs On SparkSpring device:

Intel WwanConfigurator driver passes destination buffer to memcopy that is too small:

**0:011> !analyze -v**

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**\*                                                                             \***

**\*                        Exception Analysis                                   \***

**\*                                                                             \***

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**APPLICATION\_VERIFIER\_HEAPS\_FIRST\_CHANCE\_ACCESS\_VIOLATION (13)**

**First chance access violation for current stack trace.**

**…**

**CONTEXT:  0000000c4c0fec40 -- (.cxr 0xc4c0fec40)**

**rax=00007ffa7f1b3da0 rbx=0000000000000070 rcx=00007ffa7f1b3da0**

**rdx=000001bca8562fc0 rsi=00007ffa7f1b3da0 rdi=000001bca8562fc0**

**rip=00007ffa7f11c310 rsp=0000000c4c0ff348 rbp=000001bca8562fc0**

**r8=0000000000000070  r9=000001bca8563030 r10=00007ffa7f040000**

**r11=0000000000000246 r12=0000000000000002 r13=00007ffa7f1b7b80**

**r14=0000000000000070 r15=000001bca855cfb0**

**iopl=0         nv up ei ng nz na pe cy**

**cs=0033  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00010283**

**WwanConfigurator!memcpy+0x190:**

**00007ffa`7f11c310 c4a17e6f6c02e0  vmovdqu ymm5,ymmword ptr [rdx+r8-20h] ds:000001bc`a8563010=??**

**Resetting default scope**

**…**

**0:011> k**

**# Child-SP          RetAddr               Call Site**

**00 0000000c`4c0fd6e8 00007ffa`de637cb8     ntdll!ZwWaitForMultipleObjects+0x14**

**01 0000000c`4c0fd6f0 00007ffa`de63728e     ntdll!WerpWaitForCrashReporting+0xa8**

**02 0000000c`4c0fd770 00007ffa`de636a2b     ntdll!RtlReportExceptionHelper+0x33e**

**03 0000000c`4c0fd840 00007ffa`d9592cec     ntdll!RtlReportException+0x9b**

**04 0000000c`4c0fd8c0 00007ffa`de5c7afa     vfbasics!AVrfpVectoredExceptionHandler+0x10c**

**05 0000000c`4c0fd910 00007ffa`de56e882     ntdll!RtlpCallVectoredHandlers+0x112**

**06 (Inline Function) --------`--------     ntdll!RtlCallVectoredExceptionHandlers+0xe**

**07 0000000c`4c0fd9b0 00007ffa`de5f2d5e     ntdll!RtlDispatchException+0x62**

**08 0000000c`4c0fdc00 00007ffa`d96126ee     ntdll!KiUserExceptionDispatch+0x2e**

**09 0000000c`4c0fe300 00007ffa`d961868d     vrfcore!VerifierStopMessageEx+0x81e**

**0a 0000000c`4c0fe660 00007ffa`d97b7383     vrfcore!VfCoreRedirectedStopMessage+0x8d**

**0b 0000000c`4c0fe6f0 00007ffa`de6361af     verifier!VerifierStopMessage+0xc3**

**0c 0000000c`4c0fe7a0 00007ffa`d9592853     ntdll!RtlApplicationVerifierStop+0xef**

**0d 0000000c`4c0fe810 00007ffa`d95936a0     vfbasics!VerifierStopMessage+0x223**

**0e 0000000c`4c0fe870 00007ffa`d9592bfa     vfbasics!AVrfpCheckFirstChanceException+0x148**

**0f 0000000c`4c0fe900 00007ffa`de5c7afa     vfbasics!AVrfpVectoredExceptionHandler+0x1a**

**10 0000000c`4c0fe950 00007ffa`de56e882     ntdll!RtlpCallVectoredHandlers+0x112**

**11 (Inline Function) --------`--------     ntdll!RtlCallVectoredExceptionHandlers+0xe**

**12 0000000c`4c0fe9f0 00007ffa`de5f2d5e     ntdll!RtlDispatchException+0x62**

**13 0000000c`4c0fec40 00007ffa`7f11c310     ntdll!KiUserExceptionDispatch+0x2e**

**14 0000000c`4c0ff348 00007ffa`7f090904     WwanConfigurator!memcpy+0x190**

**15 (Inline Function) --------`--------     WwanConfigurator!memcpy\_s+0x100**

**16 0000000c`4c0ff350 00007ffa`7f09ea9d     WwanConfigurator!mem\_copy+0x144**

**17 0000000c`4c0ff3f0 00007ffa`7f0832a5     WwanConfigurator!Mbim\_memcpy+0x10d**

**18 0000000c`4c0ff470 00007ffa`7f082ea9     WwanConfigurator!ril\_request\_INTC\_THERMAL\_SENSOR\_STATE\_handler+0x1f5**

**19 0000000c`4c0ff940 00007ffa`7f07fc15     WwanConfigurator!on\_request\_thermal\_handler+0x299**

**1a 0000000c`4c0ffa00 00007ffa`dc099363     WwanConfigurator!thermal\_handler+0x475**

**1b 0000000c`4c0ffae0 00007ffa`d95a786e     ucrtbase!thread\_start<unsigned int (\_\_cdecl\*)(void \*),1>+0x93**

**1c 0000000c`4c0ffb10 00007ffa`dd65244d     vfbasics!AVrfpStandardThreadFunction+0x4e**

**1d 0000000c`4c0ffb50 00007ffa`de5adf88     kernel32!BaseThreadInitThunk+0x1d**

**1e 0000000c`4c0ffb80 00000000`00000000     ntdll!RtlUserThreadStart+0x28**

**0:011> .frame /r 18**

**18 0000000c`4c0ff470 00007ffa`7f082ea9     WwanConfigurator!ril\_request\_INTC\_THERMAL\_SENSOR\_STATE\_handler+0x1f5**

**rax=3200000c4c0ff068 rbx=ffffffffffffffff rcx=00007ffade6dce20**

**rdx=0000000c4c0ff6f0 rsi=00007ffa7f13ece0 rdi=000001bca8562fc0**

**rip=00007ffa7f0832a5 rsp=0000000c4c0ff470 rbp=0000000c4c0ff570**

**r8=0000000000000001  r9=0000000c4c0ff1f0 r10=00000001de5adf00**

**r11=0000000c4c0ffb70 r12=0000000000000002 r13=00007ffa7f1b7b80**

**r14=0000000000000000 r15=000001bca855cfb0**

**iopl=0         nv up ei pl zr na po nc**

**cs=0033  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00000246**

**WwanConfigurator!ril\_request\_INTC\_THERMAL\_SENSOR\_STATE\_handler+0x1f5:**

**00007ffa`7f0832a5 41b91c000000    mov     r9d,1Ch**

**0:011> ub**

**WwanConfigurator!ril\_request\_INTC\_THERMAL\_SENSOR\_STATE\_handler+0x1d2:**

**00007ffa`7f083282 418bd1          mov     edx,r9d**

**00007ffa`7f083285 4533c0          xor     r8d,r8d**

**00007ffa`7f083288 e8a3b40100      call    WwanConfigurator!Mbim\_memset (00007ffa`7f09e730)**

**00007ffa`7f08328d 41b970000000    mov     r9d,70h**

**00007ffa`7f083293 488d0d060b1300  lea     rcx,[WwanConfigurator!set\_config (00007ffa`7f1b3da0)]**

**00007ffa`7f08329a 418bd1          mov     edx,r9d**

**00007ffa`7f08329d 4c8bc7          mov     r8,rdi**

**00007ffa`7f0832a0 e8ebb60100      call    WwanConfigurator!Mbim\_memcpy (00007ffa`7f09e990)**

**0:011> db 000001bca8562fc0 L70**

**000001bc`a8562fc0  01 00 00 00 64 00 00 00-01 00 00 00 b0 fa ff ff  ....d...........**

**000001bc`a8562fd0  14 00 00 00 e8 03 00 00-01 00 00 00 01 00 00 00  ................**

**000001bc`a8562fe0  64 00 00 00 02 00 00 00-ff ff ff ff 14 00 00 00  d...............**

**000001bc`a8562ff0  e8 03 00 00 00 00 00 00-d0 d0 d0 d0 d0 d0 d0 d0  ................**

**000001bc`a8563000  ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??  ????????????????**

**000001bc`a8563010  ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??  ????????????????**

**000001bc`a8563020  ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??  ????????????????**

**0:011> lmvi mWwanConfigurator**

**Browse full module list**

**start             end                 module name**

**00007ffa`7f040000 00007ffa`7f1de000   WwanConfigurator   (private pdb symbols)  WwanConfigurator.dll**

**Symbol file: d:\symcache\WwanConfigurator.pdb\C97089E1BCAC48008D8E450174DF4C422\WwanConfigurator.pdb**

**Image path: C:\Windows\System32\WwanConfigurator.dll**

**Image name: WwanConfigurator.dll**

**Browse all global symbols  functions  data**

**Timestamp:        Sat Oct  1 14:02:44 2022 (6338AAF4)**

**CheckSum:         00170672**

**ImageSize:        0019E000**

**File version:     0.6.200.274**

**Product version:  0.6.0.0**

**File flags:       8 (Mask 3F) Private**

**File OS:          40004 NT Win32**

**File type:        3.6 Driver**

**File date:        00000000.00000000**

**Translations:     0409.04b0**

**Information from resource tables:**

**CompanyName:      Intel(R) Corporation**

**ProductName:      Intel(R) Wwan 5G NetAdapter Stack**

**InternalName:     Intel(R) WwanConfigurator Driver"**

**OriginalFilename: WwanConfigurator.dll**

**ProductVersion:   0.6.200.274**

**FileVersion:      0.6.200.274**

**FileDescription:  Intel(R) WwanConfigurator Driver"**

**LegalCopyright:   Copyright(C), 2021 Intel Corporation. All rights reserved.**

<https://hsdes.intel.com/appstore/article/#/15012165505>

[CSPV][CSPV\_SH][CML][WHL][21H2][WOS][LKD]- LKD\_0x193\_DxgkrnlLiveDump:810\_\_dxgkrnl!DpiPowerArbiterThread\_nt!KeWaitForSingleObject\_dxgkrnl!DxgCreateLiveDumpWithWdLogs

This is VIDEO\_DXGKRNL\_LIVEDUMP - DXGKRNL\_LIVEDUMP\_DXGK\_DEADLOCK:

**0: kd> !analyze -show**

**VIDEO\_DXGKRNL\_LIVEDUMP (193)**

**Livedumps triggered by dxgkrnl**

**Arguments:**

**Arg1: 0000000000000810, Reason Code.**

**100 Internal**

**Arg2: ffffbf0d9ee85000, Reserved.**

**Arg3: ffffbf0d0dae9040, Reserved.**

**Arg4: 0000000000000458, Reserved.**

The “deadlocked” thread is the Power Arbiter for NVIDIA GFX waiting for device to go to D0:

**0: kd> !thread ffffbf0d0dae9040**

**THREAD ffffbf0d0dae9040  Cid 0004.0320  Teb: 0000000000000000 Win32Thread: 0000000000000000 WAIT: (Executive) KernelMode Non-Alertable**

**ffffbf0d0f0f10d8  SynchronizationEvent**

**Not impersonating**

**DeviceMap                 ffff80046aa361e0**

**Owning Process            ffffbf0cf26b7200       Image:         System**

**Attached Process          N/A            Image:         N/A**

**Wait Start TickCount      6561965        Ticks: 2264 (0:00:00:35.375)**

**Context Switch Count      3134           IdealProcessor: 15**

**UserTime                  00:00:00.000**

**KernelTime                00:00:00.093**

**Win32 Start Address dxgkrnl!DpiPowerArbiterThread (0xfffff8064b8e65e0)**

**Stack Init ffffba8dcd34f590 Current ffffba8dcd34f0f0**

**Base ffffba8dcd350000 Limit ffffba8dcd349000 Call 0000000000000000**

**Priority 15 BasePriority 8 PriorityDecrement 112 IoPriority 2 PagePriority 5**

**Child-SP          RetAddr               : Args to Child                                                           : Call Site**

**ffffba8d`cd34f130 fffff806`358130b0     : fffff806`2dde5180 00000000`00000000 00000000`00000000 00000000`00000000 : nt!KiSwapContext+0x76**

**ffffba8d`cd34f270 fffff806`358125df     : 00000000`00000000 00000000`0000000a ffffba8d`cd34f430 00000000`00000000 : nt!KiSwapThread+0x500**

**ffffba8d`cd34f320 fffff806`35811e83     : 00000000`00000000 ffffbf0d`00000000 00000000`00000000 ffffbf0d`0dae9180 : nt!KiCommitThreadWait+0x14f**

**ffffba8d`cd34f3c0 fffff806`4b8e6647     : ffffbf0d`0f0f10d8 00000000`00000000 00000000`00000000 ffffbf0c`f26a2100 : nt!KeWaitForSingleObject+0x233**

**ffffba8d`cd34f4b0 fffff806`35871d25     : ffffbf0d`0dae9040 00000000`00000080 fffff806`4b8e65e0 001fe47f`b19bbfff : dxgkrnl!DpiPowerArbiterThread+0x67**

**ffffba8d`cd34f510 fffff806`35a00628     : fffff806`2dde5180 ffffbf0d`0dae9040 fffff806`35871cd0 058d4809`77c03b41 : nt!PspSystemThreadStartup+0x55**

**ffffba8d`cd34f560 00000000`00000000     : ffffba8d`cd350000 ffffba8d`cd349000 00000000`00000000 00000000`00000000 : nt!KiStartSystemThread+0x28**

**0: kd> .thread /p /r ffffbf0d0dae9040**

**Implicit thread is now ffffbf0d`0dae9040**

**Implicit process is now ffffbf0c`f26b7200**

**0: kd> .frame /r 5**

**05 ffffba8d`cd34f510 fffff806`35a00628     nt!PspSystemThreadStartup+0x55**

**rax=0000000000000000 rbx=ffffbf0d0dae9040 rcx=0000000000000000**

**rdx=0000000000000000 rsi=fffff8064b8e65e0 rdi=ffffbf0d0f0f0030**

**rip=fffff80635871d25 rsp=ffffba8dcd34f510 rbp=0000000000000080**

**r8=0000000000000000  r9=0000000000000000 r10=0000000000000000**

**r11=0000000000000000 r12=0000000000000682 r13=0000000000000000**

**r14=ffffbf0cf26b7200 r15=fffff80632c16000**

**iopl=0         nv up di pl nz na pe nc**

**cs=0000  ss=0000  ds=0000  es=0000  fs=0000  gs=0000             efl=00000000**

**nt!PspSystemThreadStartup+0x55:**

**fffff806`35871d25 eb0b            jmp     nt!PspSystemThreadStartup+0x62 (fffff806`35871d32)**

**0: kd> ub**

**nt!PspSystemThreadStartup+0x3a:**

**fffff806`35871d0a 8b8310050000    mov     eax,dword ptr [rbx+510h]**

**fffff806`35871d10 83f001          xor     eax,1**

**fffff806`35871d13 83e003          and     eax,3**

**fffff806`35871d16 3c03            cmp     al,3**

**fffff806`35871d18 7518            jne     nt!PspSystemThreadStartup+0x62 (fffff806`35871d32)**

**fffff806`35871d1a 488bcf          mov     rcx,rdi**

**fffff806`35871d1d 488bc6          mov     rax,rsi**

**fffff806`35871d20 e84bfe1800      call    nt!guard\_dispatch\_icall (fffff806`35a01b70)**

**0: kd> !devstack ffffbf0d0f0f0030**

**!DevObj           !DrvObj            !DevExt           ObjectName**

**> ffffbf0d0f0f0030  \Driver\nvlddmkm   ffffbf0d0f0f0180**

**ffffbf0d018ebe00  \Driver\ACPI       ffffbf0cf26e08a0**

**ffffbf0d01cf1570  \Driver\pci        ffffbf0d01cf16c0  <???>**

**!DevNode ffffbf0cf26a16f0 :**

**DeviceInst is "PCI\VEN\_10DE&DEV\_24B8&SUBSYS\_8870103C&REV\_A1\4&2b26a038&0&0008"**

**ServiceName is "<???>"**

But NVIDIA GFX is in directed D3:

**0: kd> dt nt!\_DEVICE\_NODE ffffbf0cf26a16f0 FxDevice**

**+0x050 FxDevice : 0xffffbf0d`9efd9ad0 \_POP\_FX\_DEVICE**

**0: kd> !fxdevice 0xffffbf0d`9efd9ad0**

**!fxdevice 0xffffbf0d9efd9ad0**

**Device Object: 0xffffbf0d0f0f0030**

**DevNode: 0xffffbf0cf26a16f0**

**UniqueId: "\\_SB.PC00.PEG1.PEGP"**

**InstancePath: "PCI\VEN\_10DE&DEV\_24B8&SUBSYS\_8870103C&REV\_A1\4&2b26a038&0&0008"**

**Device Power State: PowerDeviceD3**

**PEP Owner: Default PEP**

**Acpi Plugin: 0**

**Acpi Handle: 0**

**Device Status Flags: DfxPoweredDown DevicePowerRequired**

**Device Idle Timeout: 0x0003d090**

**Device Power On: No Activity**

**Device Power Off: No Activity**

**Device Unregister: No Activity**

**…**

So NVIDIA GFX is in directed D3, therefore Power Arbiter blocks all I/O from proceeding, but Direct X Kernel times out on I/O and reports deadlock.

<https://hsdes.intel.com/appstore/article/#/13010218628>

[RPL-P682][SST][PRQ][BSOD]-CRITICAL\_PROCESS\_DIED (ef)\_svchost.exe\_BUGCHECK\_CRITICAL\_PROCESS\_6cf6b040\_systemeventsbrokerserver.dll!\_lambda\_a0c20063e4c68eb3d576b73600b3b553\_::operator()\_IMAGE\_systemeventsbrokerserver.dll:

System Events Broker is dereferencing an invalid string pointer trying to match device instance:

**2: kd> !analyze -show**

**CRITICAL\_PROCESS\_DIED (ef)**

**A critical system process died**

**Arguments:**

**Arg1: ffff860d53847080, Process object or thread object**

**Arg2: 0000000000000000, If this is 0, a process died. If this is 1, a thread died.**

**Arg3: ffff860d53847080, The process object that initiated the termination.**

**Arg4: 0000000000000000**

**2: kd> !process ffff860d53847080 0**

**PROCESS ffff860d53847080**

**SessionId: 0  Cid: 0558    Peb: a14dd92000  ParentCid: 0470**

**DirBase: 3a3e2f000  ObjectTable: ffffcf03b9096440  HandleCount: 846.**

**Image: svchost.exe**

**2: kd> k**

**# Child-SP          RetAddr               Call Site**

**00 ffff800e`afeca858 fffff804`46fa6e2b     nt!KeBugCheckEx**

**01 ffff800e`afeca860 fffff804`46ec9487     nt!PspCatchCriticalBreak+0x11b**

**02 ffff800e`afeca8f0 fffff804`46dbdd6f     nt!PspTerminateAllThreads+0x1bb7b3**

**03 ffff800e`afeca960 fffff804`46dbdb61     nt!PspTerminateProcess+0xe3**

**04 ffff800e`afeca9a0 fffff804`46a31765     nt!NtTerminateProcess+0xb1**

**05 ffff800e`afecaa20 00007ff8`bf7ef2f4     nt!KiSystemServiceCopyEnd+0x25**

**06 000000a1`4f0fe728 00007ff8`bf8767e0     ntdll!NtTerminateProcess+0x14**

**07 000000a1`4f0fe730 00007ff8`bf7f73a1     ntdll!TppWorkerpInnerExceptionFilter+0x68**

**08 000000a1`4f0fe760 00007ff8`bf7df047     ntdll!TppWorkerThread$filt$3+0x19**

**09 000000a1`4f0fe7a0 00007ff8`bf7ee896     ntdll!\_C\_specific\_handler+0x97**

**0a 000000a1`4f0fe810 00007ff8`bf7f3e1f     ntdll!\_GSHandlerCheck\_SEH+0x6a**

**0b 000000a1`4f0fe840 00007ff8`bf76eae6     ntdll!RtlpExecuteHandlerForException+0xf**

**0c 000000a1`4f0fe870 00007ff8`bf7f2e0e     ntdll!RtlDispatchException+0x286**

**0d 000000a1`4f0ff040 00007ff8`b7c0c87b     ntdll!KiUserExceptionDispatch+0x2e**

**0e (Inline Function) --------`--------     systemeventsbrokerserver!std::\_WChar\_traits<unsigned short>::length+0x16**

**0f (Inline Function) --------`--------     systemeventsbrokerserver!std::basic\_string<unsigned short,std::char\_traits<unsigned short>,std::allocator<unsigned short> >::compare+0x16**

**10 000000a1`4f0ff770 00007ff8`b7c0c7f8     systemeventsbrokerserver!<lambda\_a0c20063e4c68eb3d576b73600b3b553>::operator()+0x3b**

**11 000000a1`4f0ff780 00007ff8`b7c0c773     systemeventsbrokerserver!Broker::DeviceInterfaceArrivalEvent::MatchString<<lambda\_a0c20063e4c68eb3d576b73600b3b553> >+0x48**

**12 000000a1`4f0ff7c0 00007ff8`b7c0c645     systemeventsbrokerserver!Broker::DeviceInterfaceArrivalEvent::IsDeviceHwidPresentOnNode+0xa3**

**13 000000a1`4f0ff830 00007ff8`b7c23e4f     systemeventsbrokerserver!Broker::DeviceInterfaceArrivalEvent::IsDeviceHwidPresentOnPath+0x9d**

**14 000000a1`4f0ff8d0 00007ff8`bc8b44db     systemeventsbrokerserver!Broker::DeviceInterfaceArrivalEvent::OnDeviceNotificationArrival+0x3f**

**15 (Inline Function) --------`--------     cfgmgr32!CmNotifyCallUserCallback+0x34**

**16 000000a1`4f0ff910 00007ff8`bc8afe10     cfgmgr32!ProcessDeviceInterfaceEvent+0x93**

**17 (Inline Function) --------`--------     cfgmgr32!ProcessPlugPlayEvent+0x3d**

**18 000000a1`4f0ff960 00007ff8`bc8afcde     cfgmgr32!ProcessEventBlockList+0x70**

**19 000000a1`4f0ff9d0 00007ff8`bf7b295a     cfgmgr32!ProcessPlugPlayEventCallback+0xfe**

**1a 000000a1`4f0ffa00 00007ff8`bf786016     ntdll!TppWorkpExecuteCallback+0x13a**

**1b 000000a1`4f0ffa50 00007ff8`bd9c244d     ntdll!TppWorkerThread+0x8f6**

**1c 000000a1`4f0ffd30 00007ff8`bf7adf78     KERNEL32!BaseThreadInitThunk+0x1d**

**1d 000000a1`4f0ffd60 00000000`00000000     ntdll!RtlUserThreadStart+0x28**

**2: kd> .frame /r e**

**0e (Inline Function) --------`--------     systemeventsbrokerserver!std::\_WChar\_traits<unsigned short>::length+0x16**

**rax=0000000000000001 rbx=0000000000000015 rcx=000000a14f0ff5e0**

**rdx=a45c254e00000050 rsi=0000000000650070 rdi=000002206c8ba9c0**

**rip=00007ff8b7c0c87b rsp=000000a14f0ff770 rbp=0000000000000058**

**r8=d16720804efddf1c  r9=00000003e050a846 r10=0000000000000000**

**r11=0000000000000000 r12=0000000000000000 r13=000000000000022c**

**r14=0000000000000000 r15=0000000000000000**

**iopl=0         nv up ei pl zr na po nc**

**cs=0010  ss=0018  ds=002b  es=002b  fs=0053  gs=002b             efl=00040246**

**systemeventsbrokerserver!std::\_WChar\_traits<unsigned short>::length+0x16 [inlined in systemeventsbrokerserver!<lambda\_a0c20063e4c68eb3d576b73600b3b553>::operator()+0x3b]:**

**00007ff8`b7c0c87b 4883781808      cmp     qword ptr [rax+18h],8 ds:002b:00000000`00000019=????????????????**

**2: kd> lmvi msystemeventsbrokerserver**

**Browse full module list**

**start             end                 module name**

**00007ff8`b7c00000 00007ff8`b7c3d000   systemeventsbrokerserver # (private pdb symbols)  systemeventsbrokerserver.dll**

**Symbol file: d:\symcache\SystemEventsBrokerServer.pdb\C957647F70028873EA39309CFE373DB21\SystemEventsBrokerServer.pdb**

**Mapped memory image file: d:\symcache\systemeventsbrokerserver.dll\C65628893d000\systemeventsbrokerserver.dll**

**Image path: c:\windows\system32\systemeventsbrokerserver.dll**

**Image name: systemeventsbrokerserver.dll**

**Browse all global symbols  functions  data**

**Image was built with /Brepro flag.**

**Timestamp:        C6562889 (This is a reproducible build file hash, not a timestamp)**

**CheckSum:         00042B6A**

**ImageSize:        0003D000**

**File version:     10.0.22621.1**

**Product version:  10.0.22621.1**

**File flags:       0 (Mask 3F)**

**File OS:          40004 NT Win32**

**File type:        2.0 Dll**

**File date:        00000000.00000000**

**Translations:     0409.04b0**

**Information from resource tables:**

**CompanyName:      Microsoft Corporation**

**ProductName:      Microsoft® Windows® Operating System**

**InternalName:     SystemEventsBrokerServer.dll**

**OriginalFilename: SystemEventsBrokerServer.dll**

**ProductVersion:   10.0.22621.1**

**FileVersion:      10.0.22621.1 (WinBuild.160101.0800)**

**FileDescription:  System Events Broker**

**LegalCopyright:   © Microsoft Corporation. All rights reserved.**

<https://hsdes.intel.com/appstore/article/#/15012121700>

[SV2][KS.SYS][DriverVerifier] BSOD(LOCKED\_PAGES\_TRACKER\_CORRUPTION (d9)) occurs when preview 10 minutes in inbox.:

Kernel CSA Library (KS.SYS) can leave process pages locked or attempt to lock the same MDL twice:

**0: kd> !analyze -show**

**LOCKED\_PAGES\_TRACKER\_CORRUPTION (d9)**

**Arguments:**

**Arg1: 0000000000000001, The MDL is being inserted twice on the same process list.**

**Arg2: ffff860d6b571ca0, Address of internal lock tracking structure.**

**Arg3: ffff860d7d918fc0, Address of memory descriptor list.**

**Arg4: 0000000000006c7f, Number of pages locked for the current process.**

**0: kd> k**

**# Child-SP          RetAddr               Call Site**

**00 ffffdd87`b86def48 fffff805`2160acf9     nt!KeBugCheckEx**

**01 ffffdd87`b86def50 fffff805`2124a364     nt!MiAddMdlTracker+0x21d**

**02 ffffdd87`b86defe0 fffff805`2124aa21     nt!MiProbeAndLockComplete+0x84**

**03 ffffdd87`b86df010 fffff805`21ad3506     nt!MmProbeAndLockPages+0x91**

**04 ffffdd87`b86df110 fffff804`fd45eb30     nt!VerifierMmProbeAndLockPages+0xb6**

**05 ffffdd87`b86df150 fffff804`fd45d994     ks!KspMethodHandler+0x578**

**06 ffffdd87`b86df200 fffff804`fd45d0f7     ks!KspHandleAutomationIoControl+0x184**

**07 (Inline Function) --------`--------     ks!CKsFilter::DispatchDeviceIoControl+0x62**

**08 ffffdd87`b86df2a0 fffff804`fd415fca     ks!KsDispatchIrp+0xf7**

**09 ffffdd87`b86df360 fffff805`13b1ca0b     ks!CKsDevice::PassThroughIrp+0x6a**

**0a ffffdd87`b86df3a0 fffff805`213e0347     iacamera64+0x1ca0b**

**0b ffffdd87`b86df470 fffff805`21ab122f     nt!IopfCallDriver+0x53**

**0c ffffdd87`b86df4b0 fffff805`2144a77d     nt!IovCallDriver+0x5f**

**0d ffffdd87`b86df4f0 fffff805`05801410     nt!IofCallDriver+0x1b332d**

**0e ffffdd87`b86df530 fffff805`05801133     ksthunk!CKernelFilterDevice::DispatchIrp+0xf0**

**0f ffffdd87`b86df590 fffff805`213e0347     ksthunk!CKernelFilterDevice::DispatchIrpBridge+0x13**

**10 ffffdd87`b86df5c0 fffff805`21ab122f     nt!IopfCallDriver+0x53**

**11 ffffdd87`b86df600 fffff805`2144a77d     nt!IovCallDriver+0x5f**

**12 ffffdd87`b86df640 fffff805`216cf210     nt!IofCallDriver+0x1b332d**

**13 ffffdd87`b86df680 fffff805`216cd7dc     nt!IopSynchronousServiceTail+0x1d0**

**14 ffffdd87`b86df730 fffff805`216cbab6     nt!IopXxxControlFile+0x72c**

**15 ffffdd87`b86df940 fffff805`21437965     nt!NtDeviceIoControlFile+0x56**

**16 ffffdd87`b86df9b0 00007ffb`ef00ee54     nt!KiSystemServiceCopyEnd+0x25**

**17 000000b3`ca3fe108 00007ffb`ec40bcf5     ntdll!NtDeviceIoControlFile+0x14**

**18 000000b3`ca3fe110 00007ffb`ed1127f1     KERNELBASE!DeviceIoControl+0x125**

**19 000000b3`ca3fe180 00007ffb`80407005     KERNEL32!DeviceIoControlImplementation+0x81**

**1a 000000b3`ca3fe1d0 00007ffb`80403892     MFCORE!MFCopyPropertyStore+0x2e245**

**1b 000000b3`ca3fe260 00007ffb`7f8c66d0     MFCORE!MFCopyPropertyStore+0x2aad2**

**1c 000000b3`ca3fe2b0 00000000`00000000     IntelDeviceMFT64!DllUnregisterServer+0x2d21c0**

The MDL was freed and then re-allocated as MDL again:

**0: kd> !verifier 80 ffff860d7d918fc0 2**

**Log of recent kernel pool Allocate and Free operations:**

**There are up to 0x20000 entries in the log.**

**Parsing 0x0000000000020000 log entries, searching for address 0xffff860d7d918fc0.**

**======================================================================**

**Pool block ffff860d7d918fc0, Size 0000000000000040, Thread ffff860d760bc040**

**fffff80521ac13bc nt!VfHandlePoolAlloc+0x40c**

**fffff80521ab0e8e nt!IovAllocateMdl+0xae**

**fffff805215cc7b5 nt!DifIoAllocateMdlWrapper+0x105**

**fffff80521abaf32 nt!VerifierIoAllocateMdl+0x82**

**fffff804fd45eaf9 ks!KspMethodHandler+0x541**

**fffff804fd45d994 ks!KspHandleAutomationIoControl+0x184**

**fffff804fd45d0f7 ks!KsDispatchIrp+0xf7**

**fffff804fd415fca ks!CKsDevice::PassThroughIrp+0x6a**

**fffff80513b1ca0b iacamera64+0x1ca0b**

**fffff805213e0347 nt!IopfCallDriver+0x53**

**fffff80521ab122f nt!IovCallDriver+0x5f**

**fffff8052144a77d nt!IofCallDriver+0x1b332d**

**fffff80505801410 ksthunk!CKernelFilterDevice::DispatchIrp+0xf0**

**fffff80505801133 ksthunk!CKernelFilterDevice::DispatchIrpBridge+0x13**

**fffff805213e0347 nt!IopfCallDriver+0x53**

**fffff80521ab122f nt!IovCallDriver+0x5f**

**fffff8052144a77d nt!IofCallDriver+0x1b332d**

**fffff805216cf210 nt!IopSynchronousServiceTail+0x1d0**

**fffff805216cd7dc nt!IopXxxControlFile+0x72c**

**fffff805216cbab6 nt!NtDeviceIoControlFile+0x56**

**fffff80521437965 nt!KiSystemServiceCopyEnd+0x25**

**======================================================================**

**Pool block ffff860d7d918fc0, Size 0000000000000040, Thread ffff860d6d281080**

**fffff80521ace798 nt!VfPtFreePoolNotification+0x5c**

**fffff8052148a7b2 nt!ExpFreePoolChecks+0x1ee0a2**

**fffff805215fe027 nt!ExpFreeHeapSpecialPool+0x5f**

**fffff80521a9ed8b nt!ExFreePoolWithTag+0xd7b**

**fffff8052129d448 nt!IoFreeMdl+0x78**

**fffff805215ce920 nt!DifIoFreeMdlWrapper+0xb0**

**fffff80521abafc0 nt!VerifierIoFreeMdl+0x10**

**fffff804fd45ebf7 ks!KspMethodHandler+0x63f**

**fffff804fd45d994 ks!KspHandleAutomationIoControl+0x184**

**fffff804fd45d0f7 ks!KsDispatchIrp+0xf7**

**fffff804fd415fca ks!CKsDevice::PassThroughIrp+0x6a**

**fffff80513b1ca0b iacamera64+0x1ca0b**

**fffff805213e0347 nt!IopfCallDriver+0x53**

**fffff80521ab122f nt!IovCallDriver+0x5f**

**fffff8052144a77d nt!IofCallDriver+0x1b332d**

**fffff80505801410 ksthunk!CKernelFilterDevice::DispatchIrp+0xf0**

**fffff80505801133 ksthunk!CKernelFilterDevice::DispatchIrpBridge+0x13**

**fffff805213e0347 nt!IopfCallDriver+0x53**

**fffff80521ab122f nt!IovCallDriver+0x5f**

**fffff8052144a77d nt!IofCallDriver+0x1b332d**

**fffff805216cf210 nt!IopSynchronousServiceTail+0x1d0**

**fffff805216cd7dc nt!IopXxxControlFile+0x72c**

**fffff805216cbab6 nt!NtDeviceIoControlFile+0x56**

**fffff80521437965 nt!KiSystemServiceCopyEnd+0x25**

**Parsed 0000000000000008 entries out of 0000000000020000.**

But the previous “reincarnation” of the MDL is still inserted in the process’ Locked Pages List:

**0: kd> dt nt!\_LOCK\_TRACKER 0xffff860d6b571ca0**

**+0x000 LockTrackerNode  : \_RTL\_BALANCED\_NODE**

**+0x018 Mdl              : 0xffff860d`7d918fc0 \_MDL**

**+0x020 StartVa          : 0x000000b3`ca7fe000 Void**

**+0x028 Count            : 2**

**+0x030 Offset           : 0xf80**

**+0x034 Length           : 0x330**

**+0x038 Who              : 3**

**+0x03c Hash             : 0x89a0b6db**

**+0x040 Page             : 0x1705e2**

**+0x048 StackTrace       : [8] 0xfffff805`2160abda Void**

**+0x088 Process          : 0xffff860d`7c5d0140 \_EPROCESS**

**0: kd> dps 0xffff860d6b571ca0+48**

**ffff860d`6b571ce8  fffff805`2160abda nt!MiAddMdlTracker+0xfe**

**ffff860d`6b571cf0  fffff805`2124a364 nt!MiProbeAndLockComplete+0x84**

**ffff860d`6b571cf8  fffff805`2124aa21 nt!MmProbeAndLockPages+0x91**

**ffff860d`6b571d00  fffff805`21ad3506 nt!VerifierMmProbeAndLockPages+0xb6**

**ffff860d`6b571d08  fffff804`fd45eb30 ks!KspMethodHandler+0x578**

**ffff860d`6b571d10  fffff804`fd45d994 ks!KspHandleAutomationIoControl+0x184**

**ffff860d`6b571d18  fffff804`fd45d0f7 ks!KsDispatchIrp+0xf7**

**ffff860d`6b571d20  fffff804`fd415fca ks!CKsDevice::PassThroughIrp+0x6a**

**…**

This happens because ks!KspMethodHandler assumes that if the MDL was allocated then the only thing that can fail is probing and locking of pages.

However, if MmGetSystemAddressForMdlSafe fails, then KspMethodHandler will free the MDL without unlocking the pages.

<https://hsdes.intel.com/appstore/article/#/16018474178>

[CSPV][CSPV\_SH][ADL][21H2][BSOD]- 0x9F\_3\_Usb4HostRouter\_IMAGE\_pci.sys:

Connecting interrupts does not raise thread priority but affinitizes thread to a logical processor.

Higher priority thread than can starve interrupt connect/disconnect and effectively block power IRPs completion leading to Bugcheck 9F:

10: kd> !analyze -show

DRIVER\_POWER\_STATE\_FAILURE (9f)

A driver has failed to complete a power IRP within a specific time.

Arguments:

Arg1: 0000000000000003, A device object has been blocking an IRP for too long a time

Arg2: ffffb08c34fe6360, Physical Device Object of the stack

Arg3: ffff9e05fccbf710, nt!TRIAGE\_9F\_POWER on Win7 and higher, otherwise the Functional Device Object of the stack

Arg4: **ffffb08c4cdee390**, The blocked IRP

10: kd> !irp **ffffb08c4cdee390**

Irp is active with 6 stacks 5 is current (= 0xffffb08c4cdee580)

 No Mdl: No System Buffer: Thread 00000000:  Irp stack trace.  Pending has been returned

     cmd  flg cl Device   File     Completion-Context

 [N/A(0), N/A(0)]

            0  0 00000000 00000000 00000000-00000000

                         Args: 00000000 00000000 00000000 00000000

 [N/A(0), N/A(0)]

            0  0 00000000 00000000 00000000-00000000

                         Args: 00000000 00000000 00000000 00000000

 [N/A(0), N/A(0)]

            0  0 00000000 00000000 00000000-00000000

                         Args: 00000000 00000000 00000000 00000000

 [IRP\_MJ\_POWER(16), IRP\_MN\_WAIT\_WAKE(0)]

            0  0 ffffb08c34fe6360 00000000 00000000-00000000

               \Driver\pci

                         Args: 00000000 00000000 00000000 00000000

>[IRP\_MJ\_POWER(16), IRP\_MN\_SET\_POWER(2)]

            0 e1 **ffffb08c4a2e2da0** 00000000 fffff800245a2da0-ffffb08c4d3ec208 Success Error Cancel pending

               \Driver\Usb4HostRouter    nt!PopRequestCompletion

                         Args: 00000000 00000001 00000001 00000000

 [N/A(0), N/A(0)]

            0  0 00000000 00000000 00000000-ffffb08c4d3ec208

                         Args: 00000000 00000000 00000000 00000000

10: kd> !devstack ffffb08c4a2e2da0

  !DevObj           !DrvObj            !DevExt           ObjectName

> **ffffb08c4a2e2da0**  \Driver\Usb4HostRouterffffb08c365ea760

  ffffb08c355ead50  \Driver\ACPI       ffffb08c349e6830

  ffffb08c34fe6360  \Driver\pci        ffffb08c34fe64b0  NTPNP\_PCI0010

!DevNode ffffb08c353e8ae0 :

  DeviceInst is "PCI\VEN\_8086&DEV\_463E&SUBSYS\_896D103C&REV\_02&USB4\_MS\_CM\3&11583659&0&6A"

  ServiceName is "Usb4HostRouter"

10: kd> !wdfkd.wdfdriverinfo Usb4HostRouter

----------------------------------

Default driver image name: Usb4HostRouter

WDF library image name: Wdf01000

 FxDriverGlobals  0xffffb08c3bae6da0

 WdfBindInfo      0xfffff8004119e320

   Version        v1.33

 Library module   0xffffb08c270ec180

   ServiceName    \Registry\Machine\System\CurrentControlSet\Services\Wdf01000

   ImageName      Wdf01000

----------------------------------

WDFDRIVER: 0x00004f73bb50f318

Driver logs: !wdflogdump Usb4HostRouter.sys -d

Framework logs: !wdflogdump Usb4HostRouter.sys -f

    !wdfdevice 0x00004f73c0e14568 ff (FDO)

        Pnp/Power State: WdfDevStatePnpStarted, WdfDevStatePowerWakingConnectInterrupt, WdfDevStatePwrPolIoPresentArmedWakeCanceled

        context:  dt 0xffffb08c3f1ebd80 Usb4HostRouter!HostRouter (size is 0x168 bytes)

        EvtCleanupCallback fffff80041163580 Usb4HostRouter!WdfCpp::ObjectContext<WDFDEVICE\_\_ \*,Usb4Hrd::HostRouter,0>::EvtObjectContextCleanupThunk

        EvtDestroyCallback fffff80041162e00 Usb4HostRouter!WdfCpp::ObjectContext<WDFDEVICE\_\_ \*,Usb4Hrd::HostRouter,0>::EvtObjectContextDestroyThunk

        !wdfdevicequeues 0x00004f73c0e14568

        !wdfdevice 0x00004f73b280f4b8 ff (PDO)

            Pnp/Power State: WdfDevStatePnpStarted, WdfDevStatePowerWaitForParentArmedForWake, WdfDevStatePwrPolDx

            context:  dt 0xffffb08c4d7f0e30 Usb4HostRouter!RootDeviceRouter (size is 0x68 bytes)

            EvtDestroyCallback fffff8004117ab10 Usb4HostRouter!WdfCpp::ObjectContext<WDFDEVICE\_\_ \*,Usb4Hrd::RootDeviceRouter,0>::EvtObjectContextDestroyThunk

            !wdfdevicequeues 0x00004f73b280f4b8

        !wdfdevice 0x00004f73b600e6c8 ff (PDO)

            Pnp/Power State: WdfDevStatePnpStarted, WdfDevStatePowerWaitForParent, WdfDevStatePwrPolIoPresentArmedWakeCanceled

            context:  dt 0xffffb08c49ff1c20 Usb4HostRouter!VirtualPowerPdo (size is 0xb8 bytes)

            EvtCleanupCallback fffff8004118ed30 Usb4HostRouter!WdfCpp::ObjectContext<WDFDEVICE\_\_ \*,Usb4Hrd::VirtualPowerPdo,0>::EvtObjectContextCleanupThunk

            EvtDestroyCallback fffff8004118ece0 Usb4HostRouter!WdfCpp::ObjectContext<WDFDEVICE\_\_ \*,Usb4Hrd::VirtualPowerPdo,0>::EvtObjectContextDestroyThunk

            !wdfdevicequeues 0x00004f73b600e6c8

    !wdfdevice **0x00004f73c9a15b88** ff (FDO)

        Pnp/Power State: WdfDevStatePnpStarted, WdfDevStatePowerWakingConnectInterrupt, WdfDevStatePwrPolIoPresentArmedWakeCanceled

        context:  dt 0xffffb08c365ea760 Usb4HostRouter!HostRouter (size is 0x168 bytes)

        EvtCleanupCallback fffff80041163580 Usb4HostRouter!WdfCpp::ObjectContext<WDFDEVICE\_\_ \*,Usb4Hrd::HostRouter,0>::EvtObjectContextCleanupThunk

        EvtDestroyCallback fffff80041162e00 Usb4HostRouter!WdfCpp::ObjectContext<WDFDEVICE\_\_ \*,Usb4Hrd::HostRouter,0>::EvtObjectContextDestroyThunk

        !wdfdevicequeues 0x00004f73c9a15b88

        !wdfdevice 0x00004f73ca31ccb8 ff (PDO)

            Pnp/Power State: WdfDevStatePnpStarted, WdfDevStatePowerWaitForParentArmedForWake, WdfDevStatePwrPolDx

            context:  dt 0xffffb08c35ce3630 Usb4HostRouter!RootDeviceRouter (size is 0x68 bytes)

            EvtDestroyCallback fffff8004117ab10 Usb4HostRouter!WdfCpp::ObjectContext<WDFDEVICE\_\_ \*,Usb4Hrd::RootDeviceRouter,0>::EvtObjectContextDestroyThunk

            !wdfdevicequeues 0x00004f73ca31ccb8

        !wdfdevice 0x00004f73b890e6c8 ff (PDO)

            Pnp/Power State: WdfDevStatePnpStarted, WdfDevStatePowerWaitForParent, WdfDevStatePwrPolIoPresentArmedWakeCanceled

            context:  dt 0xffffb08c476f1c20 Usb4HostRouter!VirtualPowerPdo (size is 0xb8 bytes)

            EvtCleanupCallback fffff8004118ed30 Usb4HostRouter!WdfCpp::ObjectContext<WDFDEVICE\_\_ \*,Usb4Hrd::VirtualPowerPdo,0>::EvtObjectContextCleanupThunk

            EvtDestroyCallback fffff8004118ece0 Usb4HostRouter!WdfCpp::ObjectContext<WDFDEVICE\_\_ \*,Usb4Hrd::VirtualPowerPdo,0>::EvtObjectContextDestroyThunk

            !wdfdevicequeues 0x00004f73b890e6c8

----------------------------------

WDF Verifier settings for Usb4HostRouter.sys is OFF

----------------------------------

10: kd> !wdfdevice **0x00004f73c9a15b88** ff

Treating handle as a KMDF handle!

Dumping WDFDEVICE 0x00004f73c9a15b88

=================================

WDM PDEVICE\_OBJECTs: self **0xFFFFB08C4A2E2DA0** attached 0xFFFFB08C355EAD50 pdo 0xFFFFB08C34FE6360

Pnp state:  119 ( WdfDevStatePnpStarted )

Power state:  335 ( WdfDevStatePowerWakingConnectInterrupt )

Power Pol state:  541 ( WdfDevStatePwrPolIoPresentArmedWakeCanceled )

Default WDFIOTARGET: 00004f73c4014a78

Device is the power policy owner for the stack

No pended pnp, wait-wake irps

Pended device power !irp **0xffffb08c4cdee390** (D0)

Pnp state history:

[0] WdfDevStatePnpObjectCreated (0x100)

[1] WdfDevStatePnpInit (0x105)

[2] WdfDevStatePnpInitStarting (0x106)

[3] WdfDevStatePnpHardwareAvailable (0x108)

[4] WdfDevStatePnpEnableInterfaces (0x109)

[5] WdfDevStatePnpStarted (0x119)

owning thread:  **ffffb08cdde4f040**

Power state history:

[0] WdfDevStatePowerGotoDx (0x31a)

[1] WdfDevStatePowerNotifyingD0ExitToWakeInterrupts (0x359)

[2] WdfDevStatePowerGotoDxIoStopped (0x31c)

[3] WdfDevStatePowerDx (0x31f)

[4] WdfDevStatePowerCheckDeviceType (0x301)

[5] WdfDevStatePowerWaking (0x333)

[6] WdfDevStatePowerNotifyingD0EntryToWakeInterrupts (0x35a)

[7] WdfDevStatePowerWakingConnectInterrupt (0x335)

Power policy state history:

[0] WdfDevStatePwrPolWaitingArmedUsbSS (0x53d)

[1] WdfDevStatePwrPolWaitingArmedQueryIdle (0x53f)

[2] WdfDevStatePwrPolWaitingArmed (0x53e)

[3] WdfDevStatePwrPolWaitingArmedQueryIdle (0x53f)

[4] WdfDevStatePwrPolWaitingArmed (0x53e)

[5] WdfDevStatePwrPolWaitingArmedIoPresentCancelUsbSS (0x57f)

[6] WdfDevStatePwrPolIoPresentArmed (0x540)

[7] WdfDevStatePwrPolIoPresentArmedWakeCanceled (0x541)

Device power request history:

[0] RequestDxForIdleOut       on 2022-09-27 02:33:58.411

[1] RequestD0ForOther         on 2022-09-27 03:02:42.151

[2] RequestDxForIdleOut       on 2022-09-27 03:02:50.344

[3] RequestD0ForOther         on 2022-09-27 03:18:03.526

[4] RequestDxForIdleOut       on 2022-09-27 03:18:11.142

[5] RequestD0ForOther         on 2022-09-27 03:32:53.972

[6] RequestDxForIdleOut       on 2022-09-27 03:33:01.614

[7] RequestD0ForOther         on 2022-09-27 04:18:02.708

Idle state history:

[0] FxIdleGoingToDx (0x10)

[1] FxIdleInDx (0x11)

[2] FxIdleInDxDisabled (0x15)

[3] FxIdleInDx (0x11)

[4] FxIdleInDxIoIncrement (0x12)

[5] FxIdleInDx (0x11)

[6] FxIdleInDxIoIncrement (0x12)

[7] FxIdleInDx (0x11)

Device power requirement state history:

[0] DprDevicePowerNotRequiredD0 (0x3)

[1] DprDevicePowerNotRequiredDx (0x4)

[2] DprDevicePowerRequiredDx (0x5)

[3] DprReportingDevicePowerAvailable (0x6)

[4] DprDevicePowerRequiredD0 (0x2)

[5] DprDevicePowerNotRequiredD0 (0x3)

[6] DprDevicePowerNotRequiredDx (0x4)

[7] DprDevicePowerRequiredDx (0x5)

Power references: 2

Powered-on Children Count: 2

S0Idle policy settings:

  Idle configured and enabled, User control enabled, S0Wake capable, D3Cold supported

  IdleDxState: PowerDeviceD3

  Using system-managed idle timeout with hint

  !fxdevice -v ffffb08c4d4e48a0

  IdleTimeout: 5000 ms

  PoFx directed transition: enabled, not active

  !ddripsaction

SxWake policy settings:

  SxWake configured and enabled, User control not enabled, Arm for child

  DxState for Sx: PowerDeviceD3

Power Capabilities:

  DeviceWake[PowerSystemWorking]: DeviceWakeDepthD3cold

  DeviceWake[PowerSystemSleeping1]: DeviceWakeDepthD3hot

  DeviceWake[PowerSystemSleeping2]: DeviceWakeDepthD3hot

  DeviceWake[PowerSystemSleeping3]: DeviceWakeDepthD3hot

  DeviceWake[PowerSystemHibernate]: DeviceWakeDepthD3hot

  SystemWake: PowerSystemHibernate

  S-D mapping:

    S0->PowerDeviceD0

    S1->PowerDeviceUnspecified

    S2->PowerDeviceUnspecified

    S3->PowerDeviceD3

    S4->PowerDeviceD3

    S5->PowerDeviceD3

  IdealDxStateForSx: PowerDeviceD3

 EvtDeviceD0Entry:  Usb4HostRouter!Usb4Hrd::HostRouter::EvtDeviceD0EntryThunk (fffff80041161900)

 EvtDeviceD0EntryPostInterruptsEnabled:  Usb4HostRouter!Usb4Hrd::HostRouter::EvtDevicePostInterruptsEnabledThunk (fffff800411b82b0)

 EvtDeviceD0ExitPreInterruptsDisabled:  Usb4HostRouter!Usb4Hrd::HostRouter::EvtDevicePreInterruptsDisabledThunk (fffff800411b8390)

 EvtDeviceD0Exit:  Usb4HostRouter!Usb4Hrd::HostRouter::EvtDeviceD0ExitThunk (fffff800411b80c0)

 EvtDevicePrepareHardware:  Usb4HostRouter!Usb4Hrd::HostRouter::EvtDevicePrepareHardwareThunk (fffff800411b7c00)

 EvtDeviceReleaseHardware:  Usb4HostRouter!Usb4Hrd::HostRouter::EvtDeviceReleaseHardwareThunk (fffff800411b7eb0)

 EvtDeviceSelfManagedIoSuspend:  Usb4HostRouter!Usb4Hrd::HostRouter::EvtDeviceSelfManagedIOSuspendThunk (fffff800411b8370)

No file-object callbacks assigned

No in-caller context callbacks assigned

No preprocess callbacks assigned

No dispatch callbacks assigned

WDFCHILDLIST Handles:

 !wdfchildlist 0x00004f73bb50edd8 (static PDO list)

 !wdfchildlist 0x00004f73bb50e198

Properties:

  SynchronizationScope: WdfSynchronizationScopeNone

  ExecutionLevel: WdfExecutionLevelDispatch

  IoType (Read/Write): WdfDeviceIoBuffered

  FileObjectClass: WdfFileObjectNotRequired

  Exclusive: No

  AutoForwardCleanupClose: No

  DefaultIoPriorityBoost: 0

10: kd> !thread **ffffb08cdde4f040**

THREAD ffffb08cdde4f040  Cid 0004.65f4  Teb: 0000000000000000 Win32Thread: 0000000000000000 **READY** on processor **1**

Not impersonating

DeviceMap                 ffffc48bc9855cb0

Owning Process            ffffb08c270e3040       Image:         System

Attached Process          N/A            Image:         N/A

Wait Start TickCount      2323958        Ticks: 192 (0:00:00:03.000)

Context Switch Count      4184           IdealProcessor: 1

UserTime                  00:00:00.000

KernelTime                00:00:00.125

Win32 Start Address nt!ExpWorkerThread (0xfffff80024538ef0)

Stack Init ffff9e0602e87bb0 Current ffff9e0602e86e90

Base ffff9e0602e88000 Limit ffff9e0602e81000 Call 0000000000000000

Priority 15 BasePriority 12 PriorityDecrement 48 IoPriority 2 PagePriority 5

Child-SP          RetAddr               : Args to Child                                                           : Call Site

ffff9e06`02e86ed0 fffff800`24486fa0     : fffff800`1cd02180 ffffb08c`dde4f040 fffff800`1cd02180 00000000`00000000 : nt!KiSwapContext+0x76

ffff9e06`02e87010 fffff800`245632a6     : ffffb08c`dde4f040 ffff9e06`02e87201 00000000`00000000 ffffe780`00000001 : nt!KiProcessDeferredReadyList+0x180

ffff9e06`02e87070 fffff800`245ad24b     : ffff9e06`00000000 00000000`00000000 ffff9e06`02e87150 ffffb08c`eac56a01 : nt!KeSetSystemGroupAffinityThread+0x146

ffff9e06`02e870f0 fffff800`245ad0a0     : ffffe780`34eb9700 fffff800`00000000 00000000`00000000 ffff9e06`02e87200 : nt!KiAcquireInterruptConnectLock+0x43

ffff9e06`02e87130 fffff800`245ace70     : 00000000`00000600 00000000`00000000 ffff9e06`02e87200 ffffb08c`3feed010 : nt!KiConnectInterrupt+0x90

ffff9e06`02e871a0 fffff800`24a08726     : ffff9e06`02e87410 ffff9e06`02e87300 00000000`00000010 ffffb08c`34fe6300 : nt!KeConnectInterrupt+0x6c

ffff9e06`02e87240 fffff800`24a0836e     : ffff9e06`02e87490 ffff9e06`02e874a0 fffff800`264c2950 00000000`00000000 : nt!IopConnectInterrupt+0x33e

ffff9e06`02e87390 fffff800`264d2de5     : ffffb08c`365ea470 ffffb08c`3feed010 00000000`00000000 00000000`00000001 : nt!IoConnectInterruptEx+0x20e

ffff9e06`02e87480 fffff800`264d2c71     : ffffb08c`4d2ec1d8 00000000`00000000 ffffb08c`4d2ec020 ffff9e06`02e87650 : Wdf01000!FxInterrupt::ConnectInternal+0xd5

ffff9e06`02e87500 fffff800`264d2bfb     : ffffb08c`4d2ec1d8 ffffb08c`3deea8b0 00000000`00000000 00000000`00000004 : Wdf01000!FxInterrupt::Connect+0x61

ffff9e06`02e87590 fffff800`264cda43     : ffffb08c`3deea8b0 ffff9e06`02e87750 fffff800`26556a60 ffff9e06`02e87680 : Wdf01000!FxPkgPnp::NotifyResourceObjectsD0+0x5b

ffff9e06`02e875f0 fffff800`264d6bc7     : 00000000`00000335 fffff800`26556f00 ffffb08c`3deea8b0 00000000`00000000 : Wdf01000!FxPkgPnp::PowerWakingConnectInterrupt+0x13

ffff9e06`02e87650 fffff800`264d6d80     : fffff800`264d5f30 ffffb08c`3deea8b0 ffffb08c`3deea8b0 00000000`000003e0 : Wdf01000!FxPkgPnp::PowerEnterNewState+0x143

ffff9e06`02e877a0 fffff800`264d7052     : ffff9e06`02e87870 00000000`00000000 ffffb08c`3deeaab8 00000000`00000000 : Wdf01000!FxPkgPnp::PowerProcessEventInner+0xdc

ffff9e06`02e87820 fffff800`264d5fdd     : ffffb08c`3deeaa90 ffffb08c`3deeaab0 ffffb08c`dde4f180 00000000`00000000 : Wdf01000!FxPkgPnp::\_PowerProcessEventInner+0x32

ffff9e06`02e87850 fffff800`264d5f3c     : ffffb08c`45aea050 ffffb08c`4a2e2da0 ffffb08c`00000000 00000000`00000000 : Wdf01000!FxEventQueue::EventQueueWorker+0x95

ffff9e06`02e878a0 fffff800`24505d8b     : 00000000`397f0410 ffffb08c`475f1df0 00000000`00000000 fffff800`24f33680 : Wdf01000!FxThreadedEventQueue::\_WorkItemCallback+0xc

ffff9e06`02e878d0 fffff800`2453903f     : ffffb08c`27104c60 ffffb08c`dde4f040 ffffb08c`45aea050 00000051`00000000 : nt!IopProcessWorkItem+0xfb

ffff9e06`02e87940 fffff800`24567d95     : ffffb08c`dde4f040 ffffe780`1fcd0000 ffffb08c`dde4f040 ffffc13f`fae27f10 : nt!ExpWorkerThread+0x14f

ffff9e06`02e87b30 fffff800`2461edd4     : ffffe780`1fcc0180 ffffb08c`dde4f040 fffff800`24567d40 00000051`5c65f396 : nt!PspSystemThreadStartup+0x55

ffff9e06`02e87b80 00000000`00000000     : ffff9e06`02e88000 ffff9e06`02e81000 00000000`00000000 00000000`00000000 : nt!KiStartSystemThread+0x34

10: kd> !prcb 1

PRCB for Processor 1 at ffffe7801f99d180:

Current IRQL -- 0

Threads--  Current ffffb08cd4924040 Next 0000000000000000 Idle ffffe7801f9a9440

Processor Index 1 Number (0, 1) GroupSetMember 2

Interrupt Count -- 01a222d8

Times -- Dpc    00000093 Interrupt 00000173

         Kernel 002349a0 User      00002ced

10: kd> !thread ffffb08cd4924040

THREAD ffffb08cd4924040  Cid 0004.380c  Teb: 0000000000000000 Win32Thread: 0000000000000000 RUNNING on processor 1

Not impersonating

DeviceMap                 ffffc48bc9855cb0

Owning Process            ffffb08c270e3040       Image:         System

Attached Process          N/A            Image:         N/A

Wait Start TickCount      2316003        Ticks: 8147 (0:00:02:07.296)

Context Switch Count      101479         IdealProcessor: 12

UserTime                  00:00:00.000

KernelTime                00:04:08.859

Win32 Start Address nt!ExpWorkerThread (0xfffff80024538ef0)

Stack Init ffff9e0607387bb0 Current ffff9e0607387360

Base ffff9e0607388000 Limit ffff9e0607381000 Call 0000000000000000

Priority 16 BasePriority 7 PriorityDecrement 0 IoPriority 2 PagePriority 5

Child-SP          RetAddr               : Args to Child                                                           : Call Site

ffff9e06`07387798 fffff800`247ec2b6     : ffff8589`13ba4000 00000000`00000004 00000000`00000004 fffff800`247ebde4 : nt!RtlpFillMemoryWithInverseStride+0x101

ffff9e06`073877a0 fffff800`247eb976     : ffff8589`13ba3000 ffffb08c`4d5dfcc0 ffff8589`13ba3000 00000000`ffffffff : nt!RtlpGenericStrideWorker+0xb6

ffff9e06`07387800 fffff800`247c156c     : 00000000`00000000 ffffb08c`4d5dfcc0 ffff8589`13ba3000 ffff9f00`17e919d0 : nt!RtlScrubMemory+0xf6

ffff9e06`07387840 fffff800`247c13cd     : 00000000`00000002 ffffb08c`270e86b0 ffff9f00`17e919d0 ffffb08c`07000000 : nt!MiScrubPage+0x140

ffff9e06`07387890 fffff800`24b7f868     : ffffb08c`00000000 ffffb08c`4d5dfcc0 ffffb08c`4d5dfcd0 00000000`00000000 : nt!MiScrubNode+0x18d

ffff9e06`07387910 fffff800`2453903f     : ffffb08c`d4924040 ffffb08c`270ba670 ffffb08c`00000000 00000000`00000000 : nt!MiScrubMemoryWorker+0x28

ffff9e06`07387940 fffff800`24567d95     : ffffb08c`d4924040 ffffe780`1fcd0000 ffffb08c`d4924040 00000000`00000000 : nt!ExpWorkerThread+0x14f

ffff9e06`07387b30 fffff800`2461edd4     : ffffe780`1fcc0180 ffffb08c`d4924040 fffff800`24567d40 00000000`00000000 : nt!PspSystemThreadStartup+0x55

ffff9e06`07387b80 00000000`00000000     : ffff9e06`07388000 ffff9e06`07381000 00000000`00000000 00000000`00000000 : nt!KiStartSystemThread+0x34

<https://hsdes.intel.com/appstore/article/#/22015940905>

[CU][ADL]ADL-P\_S-4\_25217\_0xc4\_122\_VRF\_IntcAudioBus!unknown\_function hit during 1500 cycles S-4:

IntcAudioBus calls WdfWaitLockAcquire with a non-zero timeout at IRQL DISPATCH\_LEVEL:

7: kd> !analyze -show

DRIVER\_VERIFIER\_DETECTED\_VIOLATION (c4)

A device driver attempting to corrupt the system has been caught.  This is

because the driver was specified in the registry as being suspect (by the

administrator) and the kernel has enabled substantial checking of this driver.

If the driver attempts to corrupt the system, BugChecks 0xC4, 0xC1 and 0xA will

be among the most commonly seen crashes.

Arguments:

Arg1: 0000000000000122, Waiting at DISPATCH\_LEVEL, with a timeout different than zero.

Arg2: 0000000000000002, IRQL value.

Arg3: ffff930c9a498fa8, Object to wait on.

Arg4: fffffc0bc679a088, Address of the time out value.

7: kd> k

 # Child-SP          RetAddr               Call Site

00 fffffc0b`c6799508 fffff804`21d196c2     nt!DbgBreakPointWithStatus

01 fffffc0b`c6799510 fffff804`21d18ef4     nt!KiBugCheckDebugBreak+0x12

02 fffffc0b`c6799570 fffff804`21c089f7     nt!KeBugCheck2+0xc04

03 fffffc0b`c6799cf0 fffff804`21d748eb     nt!KeBugCheckEx+0x107

04 fffffc0b`c6799d30 fffff804`21bfd6db     nt!CarInitiateBugcheck+0x47

05 fffffc0b`c6799d70 fffff804`22261f00     nt!CarReportDifPluginRuleViolation+0x20b

06 fffffc0b`c6799e00 fffff804`22286bd0     nt!CarReportRuleViolationFromNt+0xe4

07 fffffc0b`c6799ea0 fffff804`22285512     nt!ViMiscValidateKeWaitUsage+0x98

08 fffffc0b`c6799f10 fffff804`21d85271     nt!VfMiscKeWaitForSingleObject\_Entry+0x22

09 fffffc0b`c6799f50 fffff804`22265b0c     nt!DifKeWaitForSingleObjectWrapper+0xd1

0a fffffc0b`c6799fe0 fffff804`22c61e30     nt!VerifierKeWaitForSingleObject+0x5c

0b (Inline Function) --------`--------     Wdf01000!MxEvent::WaitFor+0x23

0c (Inline Function) --------`--------     Wdf01000!FxWaitLockInternal::AcquireLock+0x3d

0d fffffc0b`c679a020 fffff80f`624e1131     Wdf01000!imp\_WdfWaitLockAcquire+0xa0

0e (Inline Function) --------`--------     IntcAudioBus!WdfWaitLockAcquire+0x2a

0f fffffc0b`c679a070 fffff80f`624e353c     IntcAudioBus!HDAudioBusSegment::D0Entry+0x169

10 fffffc0b`c679a0e0 fffff80f`624db8a1     IntcAudioBus!HDAudioBusSegment::SetPowerWellState+0x94

11 fffffc0b`c679a130 fffff80f`624db791     IntcAudioBus!IGfxSharedPower::SetPowerWellInt+0x8d

12 fffffc0b`c679a180 fffff80f`624db0ae     IntcAudioBus!IGfxSharedPower::SetPowerWell+0xb5

13 fffffc0b`c679a200 fffff80f`4a067bda     IntcAudioBus!IGfxSharedPower::IDispGfxFInitCb+0x13e

14 fffffc0b`c679a290 fffff80f`4a2fd1bb     dxgkrnl!DXGGLOBAL::RegisterSharedPowerComponent+0x23e

15 fffffc0b`c679a380 fffff80f`4a3b788e     dxgkrnl!DxgRegisterSharedPowerComponent+0x4f

16 fffffc0b`c679a3d0 fffff80f`4a2c7f4d     dxgkrnl!DpiSharedPowerRegister+0xe2

17 fffffc0b`c679a410 fffff80f`4a1eb1f0     dxgkrnl!DpiFdoDispatchInternalIoctl+0xa10ad

18 fffffc0b`c679a490 fffff804`21b7bd49     dxgkrnl!DpiDispatchInternalIoctl+0x100

19 fffffc0b`c679a5c0 fffff804`22266932     nt!IopfCallDriver+0x55

1a fffffc0b`c679a600 fffff804`219c5e85     nt!IovCallDriver+0x232

1b fffffc0b`c679a640 fffff80f`624dae9f     nt!IofCallDriver+0x85

1c fffffc0b`c679a680 fffff80f`624ff79d     IntcAudioBus!IGfxSharedPower::ArrivePowerWell+0xef

1d fffffc0b`c679a700 fffff804`21e752e7     IntcAudioBus!IGfxSharedPower::IDispIfaceChangePnPCallback+0x28d

1e fffffc0b`c679a770 fffff804`21e75528     nt!PnpNotifyDriverCallback+0x8f

1f fffffc0b`c679a820 fffff804`21f5ba45     nt!PnpNotifyDeviceClassChange+0x19c

20 fffffc0b`c679a8c0 fffff804`21a67cd5     nt!PnpDeviceEventWorker+0x2b5

21 fffffc0b`c679a940 fffff804`21a47097     nt!ExpWorkerThread+0x155

22 fffffc0b`c679ab30 fffff804`21c0a474     nt!PspSystemThreadStartup+0x57

23 fffffc0b`c679ab80 00000000`00000000     nt!KiStartSystemThread+0x34

IRQL is elevated:

7: kd> !irql

Debugger saved IRQL for processor 0x7 -- 2 (DISPATCH\_LEVEL)

WdfWaitLockAcquire requires PASSIVE\_LEVEL:  
“If the *Timeout* pointer is **NULL**, or if the time-out value is not zero, **WdfWaitLockAcquire** must be called at IRQL = PASSIVE\_LEVEL.”

<https://learn.microsoft.com/en-us/windows-hardware/drivers/ddi/wdfsync/nf-wdfsync-wdfwaitlockacquire>

The PDXGK\_INITIAL\_COMPONENT\_STATE callback requires DISPATCH\_LEVEL and always called at DISPATCH\_LEVEL:

typedef

    \_IRQL\_requires\_(DISPATCH\_LEVEL)

VOID

(\*PDXGK\_INITIAL\_COMPONENT\_STATE) (

    PVOID GraphicsDeviceHandle,

    PVOID PrivateHandle,

    ULONG ComponentIndex,

    BOOLEAN IsBlockingType,

    UINT InitialFState,

    GUID ComponentGuid,

    UINT PowerComponentMappingFlag

);

This is a programmatic error in IntcAudioBus.sys.

<https://hsdes.intel.com/appstore/article/#/16018383691>

[RPL-P][DC4][HLK][SV2][Audio][ACX]: "System - PNP (disable and enable) with IO Before and After (Reliability)" test is failing due to Unexpected Reboot and dump is showing Bugcheck-0xC4 (DRIVER\_VERIFIER\_DETECTED\_VIOLATION) pointing to SdcaHid.sys:

This is a memory leak in SoundWire HID Driver (SdcaHid.sys) see attached memory dump:

**7: kd> !analyze -show**

**DRIVER\_VERIFIER\_DETECTED\_VIOLATION (c4)**

**A device driver attempting to corrupt the system has been caught.  This is**

**because the driver was specified in the registry as being suspect (by the**

**administrator) and the kernel has enabled substantial checking of this driver.**

**If the driver attempts to corrupt the system, BugChecks 0xC4, 0xC1 and 0xA will**

**be among the most commonly seen crashes.**

**Arguments:**

**Arg1: 0000000000000062, A driver has forgotten to free its pool allocations prior to unloading.**

**Arg2: ffff99034d92bc70, name of the driver having the issue.**

**Arg3: ffff990367339150, verifier internal structure with driver information.**

**Arg4: 0000000000000005, total # of (paged+nonpaged) allocations that weren't freed.**

**Type !verifier 3 drivername.sys for info on the allocations**

**that were leaked that caused the bugcheck.**

**7: kd> du ffff99034d92bc70**

**ffff9903`4d92bc70  "SdcaHid.sys"**

**7: kd> !verifier 3 SdcaHid.sys**

**Verify Flags Level 0x00100999**

**STANDARD FLAGS:**

**[X] (0x00000000) Automatic Checks**

**[X] (0x00000001) Special pool**

**[ ] (0x00000002) Force IRQL checking**

**[X] (0x00000008) Pool tracking**

**[X] (0x00000010) I/O verification**

**[ ] (0x00000020) Deadlock detection**

**[X] (0x00000080) DMA checking**

**[X] (0x00000100) Security checks**

**[X] (0x00000800) Miscellaneous checks**

**[ ] (0x00020000) DDI compliance checking**

**ADDITIONAL FLAGS:**

**[ ] (0x00000004) Randomized low resources simulation**

**[ ] (0x00000200) Force pending I/O requests**

**[ ] (0x00000400) IRP logging**

**[ ] (0x00002000) Invariant MDL checking for stack**

**[ ] (0x00004000) Invariant MDL checking for driver**

**[ ] (0x00008000) Power framework delay fuzzing**

**[ ] (0x00010000) Port/miniport interface checking**

**[ ] (0x00040000) Systematic low resources simulation**

**[ ] (0x00080000) DDI compliance checking (additional)**

**[ ] (0x00200000) NDIS/WIFI verification**

**[ ] (0x00800000) Kernel synchronization delay fuzzing**

**[ ] (0x01000000) VM switch verification**

**[ ] (0x02000000) Code integrity checks**

**RESERVED FLAGS (use of these flags is unsupported):**

**[X] (0x00100000) Unused or reserved flag**

**[X] Indicates flag is enabled**

**Summary of All Verifier Statistics**

**RaiseIrqls           0x0**

**AcquireSpinLocks     0x0**

**Synch Executions     0x0**

**Trims                0x0**

**Pool Allocations Attempted             0x106dca**

**Pool Allocations Succeeded             0x106dca**

**Pool Allocations Succeeded SpecialPool 0x106dca**

**Pool Allocations With NO TAG           0x0**

**Pool Allocations Failed                0x0**

**Current paged pool allocations         0x3001 for 00B3CADF bytes**

**Peak paged pool allocations            0x311c for 0188A490 bytes**

**Current nonpaged pool allocations      0x1484c for 0BBDD2B0 bytes**

**Peak nonpaged pool allocations         0x15742 for 0C4331B0 bytes**

**Driver Verification List**

**------------------------**

**nt!\_VF\_TARGET\_DRIVER 0xffff9903673af390: sdcahid.sys (Loaded)**

**Pool Allocation Statistics: ( NonPagedPool / PagedPool )**

**Current Pool Allocations: ( 0x00000005 / 0x00000000 )**

**Current Pool Bytes:       ( 0x0000005c / 0x00000000 )**

**Peak Pool Allocations:    ( 0x00000016 / 0x00000005 )**

**Peak Pool Bytes:          ( 0x00000eb1 / 0x000000ca )**

**Contiguous Memory Bytes:       0x00000000**

**Peak Contiguous Memory Bytes:  0x00000000**

**Pool Allocations:**

**Address             Length      Tag   Caller Address**

**------------------  ----------  ----  ------------------**

**0xffff99036a5b4ff0  0x00000005  SWUm  0xfffff805bdcc1038  SdcaHid+0x1038**

**0xffff99036a5b2ff0  0x00000005  SWUm  0xfffff805bdcc1038  SdcaHid+0x1038**

**0xffff99036a5b0ff0  0x00000005  SWUm  0xfffff805bdcc1038  SdcaHid+0x1038**

**0xffff99036a5aeff0  0x00000005  SWUm  0xfffff805bdcc1038  SdcaHid+0x1038**

**0xffff99036a5a0fb0  0x00000048  SWHi  0xfffff805bdcc1038  SdcaHid+0x1038**

**Contiguous allocations are not displayed with public symbols.**

<https://hsdes.intel.com/appstore/article/#/16018383666>

[RPL-P][DC4][HLK][SV2][Audio][ACX]: "System - PNP (disable and enable) with IO Before and After (Reliability)" test is failing due to Unexpected Reboot and dump showing Bugcheck-0xCA (PNP\_DETECTED\_FATAL\_ERROR) pointing to SdcaClassV06.sys:

SoundWire Device Class for Audio Class Driver (SdcaClassV06.sys) passes invalid PDO device object to  nt!IoReportTargetDeviceChangeAsynchronous (<https://learn.microsoft.com/en-us/windows-hardware/drivers/ddi/wdm/nf-wdm-ioreporttargetdevicechangeasynchronous>) – see attached memory dump:

**18: kd> !analyze -show**

**PNP\_DETECTED\_FATAL\_ERROR (ca)**

**PnP encountered a severe error, either as a result of a problem in a driver or**

**a problem in PnP itself.  The first argument describes the nature of the**

**problem, the second argument is the address of the PDO.  The other arguments**

**vary depending on argument 1.**

**Arguments:**

**Arg1: 0000000000000002, Invalid PDO**

**An API which requires a PDO has been called with either an FDO,**

**a PDO which hasn't been initialized yet (returned to PnP in a**

**QueryDeviceRelation/BusRelations), or some random piece of**

**memory.**

**Arg2: 0000000000000000, Purported PDO.**

**Arg3: 0000000000000000, Driver object.**

**Arg4: 0000000000000000**

**18: kd> k**

**# Child-SP          RetAddr               Call Site**

**00 fffff48c`3169d728 fffff803`4b0673e6     nt!KeBugCheckEx**

**01 fffff48c`3169d730 fffff802`d2608c4a     nt!IoReportTargetDeviceChangeAsynchronous+0x260a26**

**02 fffff48c`3169d780 fffff802`d26067b9     SdcaClassV06+0x28c4a**

**03 fffff48c`3169d7f0 fffff802`d26061c2     SdcaClassV06+0x267b9**

**04 fffff48c`3169d860 fffff802`9e0f7c70     SdcaClassV06+0x261c2**

**05 fffff48c`3169d960 fffff802`9e0eaf51     Acx01000!Acx::AfxHelper::DispatchProperty+0x130**

**06 fffff48c`3169da10 fffff802`9e0eadf0     Acx01000!Acx::AfxCircuit::DispatchRequest+0x155**

**07 fffff48c`3169dac0 fffff802`9e0eab33     Acx01000!Acx::AfxCircuit::DispatchRequestToTarget+0x230**

**08 fffff48c`3169db70 fffff802`9e0f7b34     Acx01000!Acx::AfxCircuit::EvtQueueIoDeviceControlHandler+0x133**

**09 fffff48c`3169dbe0 fffff803`4ae975ca     Acx01000!Acx::AfxHelper::AfxExpandStackIoCtrlHandler\_Thunk+0x24**

**0a fffff48c`3169dc20 fffff803`4af95985     nt!KeExpandKernelStackAndCalloutInternal+0x7a**

**0b fffff48c`3169dc90 fffff802`9e0f7a73     nt!KeExpandKernelStackAndCallout+0x15**

**0c fffff48c`3169dcd0 fffff802`9e0ea9c2     Acx01000!Acx::AfxHelper::AfxExpandStackIoCtrlHandler+0x4f**

**0d fffff48c`3169dd60 fffff803`4bf0525b     Acx01000!Acx::AfxCircuit::EvtQueueIoDeviceControlHandler\_ExpandStack+0x22**

**0e (Inline Function) --------`--------     Wdf01000!FxIoQueueIoDeviceControl::Invoke+0x44**

**0f fffff48c`3169ddb0 fffff803`4bf04f06     Wdf01000!FxIoQueue::DispatchRequestToDriver+0x16b**

**10 fffff48c`3169de20 fffff803`4bf662a8     Wdf01000!FxIoQueue::DispatchEvents+0x216**

**11 fffff48c`3169dea0 fffff803`4bf0f905     Wdf01000!FxIoQueue::QueueRequest+0x1bc**

**12 fffff48c`3169df00 fffff803`4bf0d29c     Wdf01000!FxPkgIo::DispatchStep2+0x1ff**

**13 fffff48c`3169df60 fffff802`9e0e63b3     Wdf01000!imp\_WdfDeviceWdmDispatchIrpToIoQueue+0x17c**

**14 (Inline Function) --------`--------     Acx01000!WdfDeviceWdmDispatchIrpToIoQueue+0x2b**

**15 fffff48c`3169dfc0 fffff803`4bf12eda     Acx01000!Acx::AfxDevice::EvtDeviceWdmIrpDispatch+0x223**

**16 fffff48c`3169e020 fffff803`4bf042ce     Wdf01000!FxPkgIo::DispatchStep1+0xebfa**

**17 fffff48c`3169e0f0 fffff803`4bf3dfee     Wdf01000!FxPkgIo::Dispatch+0x5e**

**18 fffff48c`3169e150 fffff803`4bf3df35     Wdf01000!DispatchWorker+0x9a**

**19 fffff48c`3169e180 fffff803`4bf34418     Wdf01000!FxDevice::DispatchPreprocessedIrp+0xa1**

**1a fffff48c`3169e1c0 fffff802`9e0e6fbb     Wdf01000!imp\_WdfDeviceWdmDispatchIrp+0xb8**

**1b (Inline Function) --------`--------     Acx01000!WdfDeviceWdmDispatchIrp+0x24**

**1c fffff48c`3169e1f0 fffff803`4bf3e783     Acx01000!AfxEvtIrpPreprocessDeviceIoCtrl+0x19b**

**1d fffff48c`3169e240 fffff803`4bf0b924     Wdf01000!PreprocessIrp+0x63**

**1e (Inline Function) --------`--------     Wdf01000!DispatchWorker+0x3e11**

**1f (Inline Function) --------`--------     Wdf01000!FxDevice::Dispatch+0x3e20**

**20 fffff48c`3169e270 fffff803`4afdb997     Wdf01000!FxDevice::DispatchWithLock+0x3e64**

**21 fffff48c`3169e2c0 fffff803`4b6ad3f0     nt!IopfCallDriver+0x53**

**22 fffff48c`3169e300 fffff803`4b04557d     nt!IovCallDriver+0x230**

**23 fffff48c`3169e340 fffff802`9e031410     nt!IofCallDriver+0x1b1fcd**

**24 fffff48c`3169e380 fffff802`9e031133     ksthunk!CKernelFilterDevice::DispatchIrp+0xf0**

**25 fffff48c`3169e3e0 fffff803`4afdb997     ksthunk!CKernelFilterDevice::DispatchIrpBridge+0x13**

**26 fffff48c`3169e410 fffff803`4b6ad3f0     nt!IopfCallDriver+0x53**

**27 fffff48c`3169e450 fffff803`4b04557d     nt!IovCallDriver+0x230**

**28 fffff48c`3169e490 fffff803`4bf09452     nt!IofCallDriver+0x1b1fcd**

**29 fffff48c`3169e4d0 fffff803`4bf53e5d     Wdf01000!FxIoTarget::Send+0x12**

**2a fffff48c`3169e500 fffff803`4bf0b6ff     Wdf01000!FxIoTarget::SubmitSync+0x1f5**

**2b fffff48c`3169e5c0 fffff802`9b958627     Wdf01000!imp\_WdfRequestSend+0x5bff**

**2c fffff48c`3169e620 fffff802`9b954013     SdcaAggregator+0x18627**

**2d fffff48c`3169e700 fffff802`9b954435     SdcaAggregator+0x14013**

**2e fffff48c`3169e780 fffff802`9e0f7c70     SdcaAggregator+0x14435**

**2f fffff48c`3169e890 fffff802`9e0eaf51     Acx01000!Acx::AfxHelper::DispatchProperty+0x130**

**30 fffff48c`3169e940 fffff802`9e0eadf0     Acx01000!Acx::AfxCircuit::DispatchRequest+0x155**

**31 fffff48c`3169e9f0 fffff802`9e0eeec9     Acx01000!Acx::AfxCircuit::DispatchRequestToTarget+0x230**

**32 fffff48c`3169eaa0 fffff802`9b953c6e     Acx01000!imp\_AcxCircuitDispatchAcxRequest+0x139**

**33 fffff48c`3169eb00 fffff802`9e0eab26     SdcaAggregator+0x13c6e**

**34 fffff48c`3169ed20 fffff802`9e0f7b34     Acx01000!Acx::AfxCircuit::EvtQueueIoDeviceControlHandler+0x126**

**35 fffff48c`3169ed90 fffff803`4ae975ca     Acx01000!Acx::AfxHelper::AfxExpandStackIoCtrlHandler\_Thunk+0x24**

**36 fffff48c`3169edd0 fffff803`4af95985     nt!KeExpandKernelStackAndCalloutInternal+0x7a**

**37 fffff48c`3169ee40 fffff802`9e0f7a73     nt!KeExpandKernelStackAndCallout+0x15**

**38 fffff48c`3169ee80 fffff802`9e0ea9c2     Acx01000!Acx::AfxHelper::AfxExpandStackIoCtrlHandler+0x4f**

**39 fffff48c`3169ef10 fffff803`4bf0525b     Acx01000!Acx::AfxCircuit::EvtQueueIoDeviceControlHandler\_ExpandStack+0x22**

**3a (Inline Function) --------`--------     Wdf01000!FxIoQueueIoDeviceControl::Invoke+0x44**

**3b fffff48c`3169ef60 fffff803`4bf04f06     Wdf01000!FxIoQueue::DispatchRequestToDriver+0x16b**

**3c fffff48c`3169efd0 fffff803`4bf662a8     Wdf01000!FxIoQueue::DispatchEvents+0x216**

**3d fffff48c`3169f050 fffff803`4bf0f905     Wdf01000!FxIoQueue::QueueRequest+0x1bc**

**3e fffff48c`3169f0b0 fffff803`4bf0d29c     Wdf01000!FxPkgIo::DispatchStep2+0x1ff**

**3f fffff48c`3169f110 fffff802`9e0e63b3     Wdf01000!imp\_WdfDeviceWdmDispatchIrpToIoQueue+0x17c**

**40 (Inline Function) --------`--------     Acx01000!WdfDeviceWdmDispatchIrpToIoQueue+0x2b**

**41 fffff48c`3169f170 fffff803`4bf12eda     Acx01000!Acx::AfxDevice::EvtDeviceWdmIrpDispatch+0x223**

**42 fffff48c`3169f1d0 fffff803`4bf042ce     Wdf01000!FxPkgIo::DispatchStep1+0xebfa**

**43 fffff48c`3169f2a0 fffff803`4bf3dfee     Wdf01000!FxPkgIo::Dispatch+0x5e**

**44 fffff48c`3169f300 fffff803`4bf3df35     Wdf01000!DispatchWorker+0x9a**

**45 fffff48c`3169f330 fffff803`4bf34418     Wdf01000!FxDevice::DispatchPreprocessedIrp+0xa1**

**46 fffff48c`3169f370 fffff802`9e0e6fbb     Wdf01000!imp\_WdfDeviceWdmDispatchIrp+0xb8**

**47 (Inline Function) --------`--------     Acx01000!WdfDeviceWdmDispatchIrp+0x24**

**48 fffff48c`3169f3a0 fffff803`4bf3e783     Acx01000!AfxEvtIrpPreprocessDeviceIoCtrl+0x19b**

**49 fffff48c`3169f3f0 fffff803`4bf0b924     Wdf01000!PreprocessIrp+0x63**

**4a (Inline Function) --------`--------     Wdf01000!DispatchWorker+0x3e11**

**4b (Inline Function) --------`--------     Wdf01000!FxDevice::Dispatch+0x3e20**

**4c fffff48c`3169f420 fffff803`4afdb997     Wdf01000!FxDevice::DispatchWithLock+0x3e64**

**4d fffff48c`3169f470 fffff803`4b6ad21f     nt!IopfCallDriver+0x53**

**4e fffff48c`3169f4b0 fffff803`4b04557d     nt!IovCallDriver+0x5f**

**4f fffff48c`3169f4f0 fffff802`9e031410     nt!IofCallDriver+0x1b1fcd**

**50 fffff48c`3169f530 fffff802`9e031133     ksthunk!CKernelFilterDevice::DispatchIrp+0xf0**

**51 fffff48c`3169f590 fffff803`4afdb997     ksthunk!CKernelFilterDevice::DispatchIrpBridge+0x13**

**52 fffff48c`3169f5c0 fffff803`4b6ad21f     nt!IopfCallDriver+0x53**

**53 fffff48c`3169f600 fffff803`4b04557d     nt!IovCallDriver+0x5f**

**54 fffff48c`3169f640 fffff803`4b2caf70     nt!IofCallDriver+0x1b1fcd**

**55 fffff48c`3169f680 fffff803`4b2c953c     nt!IopSynchronousServiceTail+0x1d0**

**56 fffff48c`3169f730 fffff803`4b2c7816     nt!IopXxxControlFile+0x72c**

**57 fffff48c`3169f940 fffff803`4b032765     nt!NtDeviceIoControlFile+0x56**

**58 fffff48c`3169f9b0 00007ffa`0812ee54     nt!KiSystemServiceCopyEnd+0x25**

**59 00000045`0e3ff0d8 00007ffa`0561bcbb     ntdll!NtDeviceIoControlFile+0x14**

**5a 00000045`0e3ff0e0 00007ffa`079427f1     KERNELBASE!DeviceIoControl+0x6b**

**5b 00000045`0e3ff150 00007ff9`f31a2074     KERNEL32!DeviceIoControlImplementation+0x81**

**5c 00000045`0e3ff1a0 00007ff9`f31a4fac     MMDevApi!HrIoctl+0x64**

**5d 00000045`0e3ff210 00007ff9`f33d2b55     MMDevApi!CKsFilterProperty::KsProperty+0x6c**

**5e 00000045`0e3ff260 00007ff9`f33b6de7     audioendpointbuilder!SetOrientationProperty+0x495**

**5f 00000045`0e3ff350 00007ff9`f339f28a     audioendpointbuilder!CAvEndpointBuilder::SetEndpointActive+0x1bb17**

**60 00000045`0e3ff460 00007ff9`f339d0a1     audioendpointbuilder!CAvEndpointBuilder::EndpointRTM+0x206a**

**61 00000045`0e3ffa80 00007ff9`f339bd0d     audioendpointbuilder!CAvEndpointBuilder::SyncEndpointInternal+0x12c1**

**62 00000045`0e3ffc10 00007ff9`f339bb89     audioendpointbuilder!CAvEndpointBuilder::SyncEndpoint+0x8d**

**63 00000045`0e3ffc70 00007ff9`f33d0e30     audioendpointbuilder!CAvEndpointBuilder::SyncEndpoints+0x189**

**64 00000045`0e3ffce0 00007ff9`f33bf959     audioendpointbuilder!CAvEndpointBuilder::OnDeviceInterfaceRemoval+0x7cc**

**65 00000045`0e3ffe10 00007ff9`f33bf1a6     audioendpointbuilder!VAD\_EndpointBuilderAudioInterfaceRemoval+0x19**

**66 00000045`0e3ffe40 00007ff9`f33b19dd     audioendpointbuilder!CAudioEpbService::DeviceRemovalEvent+0x116**

**67 00000045`0e3ffe70 00007ff9`f33a8357     audioendpointbuilder!DEVICE\_EVENT::Invoke+0x81dd**

**68 00000045`0e3ffea0 00007ffa`0795244d     audioendpointbuilder!EventWorkerThread+0x97**

**69 00000045`0e3ffee0 00007ffa`080edf78     KERNEL32!BaseThreadInitThunk+0x1d**

**6a 00000045`0e3fff10 00000000`00000000     ntdll!RtlUserThreadStart+0x28**