<https://hsdes.intel.com/appstore/article/#/16022282245>

[EGS][XCC-8S][Multisocket]- Bug check 0xA observed while reboot or shutdown in 8S system with SGX enabled:

This issue is caused by the Intel Software Guard Extensions Launch Control Configuration Service driver (sgx\_lc\_msr.sys).

In its FLCMSREvtDeviceD0Exit routine, the driver frees the memory backing an already queued DPC – this creates a race condition and when DPC queue is drained, the OS hits #PF exception because the memory for the DPC has been freed already and no longer valid. An unhandled exception in kernel mode requires OS to stop, hence the Bugcheck.

This issue should be dispatched and investigated by the owners of the sgx\_lc\_msr.sys driver – platf\_win\_os.bug HSD-ES database is for Windows OS software issues only.

This bug can cause other data/memory corruption signatures, so any of such issues should be reproduced with sgx\_lc\_msr.sys disabled to avoid duplication.

This is what happened – an invalid memory was referenced:

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

**IRQL\_NOT\_LESS\_OR\_EQUAL (a)**

**An attempt was made to access a pageable (or completely invalid) address at an**

**interrupt request level (IRQL) that is too high.  This is usually**

**caused by drivers using improper addresses.**

**If a kernel debugger is available get the stack backtrace.**

**Arguments:**

**Arg1: ffffd20edee20108, memory referenced**

**Arg2: 00000000000000ff, IRQL**

**Arg3: 0000000000000000, bitfield :**

**bit 0 : value 0 = read operation, 1 = write operation**

**bit 3 : value 0 = not an execute operation, 1 = execute operation (only on chips which support this level of status)**

**Arg4: fffff8075c8f0821, address which referenced memory**

**740: kd> !pte ffffd20edee20108**

**VA ffffd20edee20108**

**PXE at FFFFF9FCFE7F3D20    PPE at FFFFF9FCFE7A41D8    PDE at FFFFF9FCF483B7B8    PTE at FFFFF9E9076F7100**

**contains 0A0000000086C863  contains 0A0000000086D863  contains 0000000000000000**

**pfn 86c       ---DA--KWEV  pfn 86d       ---DA--KWEV  contains 0000000000000000**

**not valid**

This happened as OS was draining the DPC queue:

**740: kd> k**

**# Child-SP          RetAddr               Call Site**

**00 ffffcd01`888b6698 fffff807`5cb67152     nt!DbgBreakPointWithStatus**

**01 ffffcd01`888b66a0 fffff807`5cb669c1     nt!KiBugCheckDebugBreak+0x12**

**02 ffffcd01`888b6700 fffff807`5ca2dcf7     nt!KeBugCheck2+0xa61**

**03 ffffcd01`888b6e60 fffff807`5ca42f69     nt!KeBugCheckEx+0x107**

**04 ffffcd01`888b6ea0 fffff807`5ca3e74c     nt!KiBugCheckDispatch+0x69**

**05 ffffcd01`888b6fe0 fffff807`5c8f0821     nt!KiPageFault+0x44c**

**06 ffffcd01`888b7170 fffff807`5c9d89be     nt!KiExecuteAllDpcs+0x611**

**07 ffffcd01`888b7350 fffff807`5c9661d5     nt!KiExecuteDpc+0xbe**

**08 ffffcd01`888b74b0 fffff807`5ca32b08     nt!PspSystemThreadStartup+0x55**

**09 ffffcd01`888b7500 00000000`00000000     nt!KiStartSystemThread+0x28**

The memory for the DPC was freed already by the sgx\_lc\_msr.sys driver:

**740: kd> !verifier 80 ffffd20edee20108 1**

**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 0xffffd20edee20108.**

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

**Pool block ffffd20edee13000, Size 0000000000011000, Thread ffffd80c4a239040**

**fffff8075d084ef8 nt!VfPtFreePoolNotification+0x5c**

**fffff8075ca5026c nt!ExFreeHeapPool+0x20bc1c**

**fffff8075d055019 nt!ExFreePool+0x9**

**fffff8075cbfe94a nt!DifExFreePoolWithTagWrapper+0xca**

**fffff8075d06609c nt!VerifierExFreePoolWithTag+0x4c**

**fffff804d7217914 sgx\_lc\_msr!FLCMSREvtDeviceD0Exit+0xd4**

**fffff8075deae443 Wdf01000!FxPnpDeviceD0Exit::InvokeClient+0x23**

**fffff8075dead4a6 Wdf01000!FxPrePostCallback::InvokeStateless+0x32**

**fffff8075dea2431 Wdf01000!FxPkgPnp::PowerGotoDxIoStoppedCommon+0xf1**

**fffff8075deae9eb Wdf01000!FxPkgPnp::PowerGotoDNotZeroIoStopped+0xb**

**fffff8075dea7aff Wdf01000!FxPkgPnp::PowerEnterNewState+0x143**

**fffff8075dea7cb4 Wdf01000!FxPkgPnp::PowerProcessEventInner+0xd8**

**fffff8075dea8662 Wdf01000!FxPkgPnp::PowerProcessEvent+0x142**

**Parsed 000000000000006b entries out of 0000000000020000.**

<https://hsdes.intel.com/appstore/article/#/22018926164>

[TSE][LNL] Windows OS crash after enabling driver verifier on TSE driver version 1058 (wrong IRQL used in WDF function call):

**This is DRIVER\_VERIFIER\_DETECTED\_VIOLATION (c4) (see attached memory dump):**

1: 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: 0000000000000001, caller is trying to allocate paged pool at DISPATCH\_LEVEL or above

Arg2: 0000000000000002, current IRQL

Arg3: 0000000000000401, pool type

Arg4: 0000000000000018, number of bytes

**Current IRQL is DISPATCH\_LEVEL:**

1: kd> !irql

Debugger saved IRQL for processor 0x1 -- 2 (DISPATCH\_LEVEL)

**TSE.SYS is calling ExAllocatePool2:**

**1: kd> k**

**# Child-SP          RetAddr               Call Site**

**00 ffff8c0a`643f66b8 fffff800`42be9232     nt!DbgBreakPointWithStatus**

**01 ffff8c0a`643f66c0 fffff800`42be88e2     nt!KiBugCheckDebugBreak+0x12**

**02 ffff8c0a`643f6720 fffff800`42a45707     nt!KeBugCheck2+0xb22**

**03 ffff8c0a`643f6e90 fffff800`42c5a167     nt!KeBugCheckEx+0x107**

**04 ffff8c0a`643f6ed0 fffff800`42c58559     nt!CarInitiateBugcheck+0x47**

**05 ffff8c0a`643f6f10 fffff800`431681e8     nt!CarReportDifPluginRuleViolation+0x199**

**06 ffff8c0a`643f6fa0 fffff800`43181781     nt!CarReportRuleViolationFromNt+0xe4**

**07 ffff8c0a`643f7040 fffff800`4316befd     nt!ExAllocatePoolSanityChecks+0x195**

**08 ffff8c0a`643f7090 fffff800`42c5c706     nt!VfHandlePoolAlloc+0xfd**

**09 ffff8c0a`643f7130 fffff800`4316b9aa     nt!DifExAllocatePool2Wrapper+0xf6**

**0a ffff8c0a`643f7200 fffff800`44b119f1     nt!VerifierExAllocatePool2+0x10a**

**0b ffff8c0a`643f7270 fffff800`44b11cb0     TSE+0x19f1**

**0c ffff8c0a`643f74f0 fffff800`44b145bd     TSE+0x1cb0**

**0d ffff8c0a`643f7550 fffff800`4443ab88     TSE+0x45bd**

**0e ffff8c0a`643f75f0 fffff800`443eb267     Wdf01000!FxPnpDevicePrepareHardware::InvokeClient+0x28**

**0f ffff8c0a`643f7640 fffff800`44414404     Wdf01000!FxPrePostCallback::InvokeStateful+0x5b**

**10 (Inline Function) --------`--------     Wdf01000!FxPnpDevicePrepareHardware::Invoke+0x51**

**11 ffff8c0a`643f7680 fffff800`4441427a     Wdf01000!FxPkgPnp::PnpPrepareHardware+0xf8**

**12 ffff8c0a`643f76d0 fffff800`44428eba     Wdf01000!FxPkgPnp::PnpEventHardwareAvailable+0x5a**

**13 ffff8c0a`643f7710 fffff800`44428bd0     Wdf01000!FxPkgPnp::PnpEnterNewState+0x126**

**14 ffff8c0a`643f77b0 fffff800`44428892     Wdf01000!FxPkgPnp::PnpProcessEventInner+0xe0**

**15 ffff8c0a`643f7830 fffff800`4441ccc3     Wdf01000!FxPkgPnp::\_PnpProcessEventInner+0x32**

**16 ffff8c0a`643f7860 fffff800`4441cba5     Wdf01000!FxEventQueue::EventQueueWorker+0x9b**

**17 ffff8c0a`643f78b0 fffff800`429260b1     Wdf01000!FxWorkItemEventQueue::\_WorkItemCallback+0x25**

**18 ffff8c0a`643f78e0 fffff800`42921fe5     nt!IopProcessWorkItem+0x141**

**19 ffff8c0a`643f7950 fffff800`429ab4f7     nt!ExpWorkerThread+0x155**

**1a ffff8c0a`643f7b30 fffff800`42a8f274     nt!PspSystemThreadStartup+0x57**

**1b ffff8c0a`643f7b80 00000000`00000000     nt!KiStartSystemThread+0x34**

**Switching to the caller’s frame and disassembling backwards, we can see pool flags passed:**

1: kd> .frame /r b

0b ffff8c0a`643f7270 fffff800`44b11cb0     TSE+0x19f1

rax=0000000000000000 rbx=0000000000000000 rcx=0000000000000003

rdx=000000000000008a rsi=ffffe18a99386458 rdi=0000000000000000

rip=fffff80044b119f1 rsp=ffff8c0a643f7270 rbp=ffff8c0a643f7300

 r8=0000000000000065  r9=0000000000000000 r10=0000000000000000

r11=0000000000000000 r12=0000000000000008 r13=fffff80044b191d0

r14=0000000000000018 r15=fffff80044b1b008

iopl=0         nv up ei ng nz na po nc

cs=0010  ss=0018  ds=002b  es=002b  fs=0053  gs=002b             efl=00040286

TSE+0x19f1:

fffff800`44b119f1 4c8bc0          mov     r8,rax

**The flags indicated POOL\_FLAG\_PAGED:**

1: kd> ub

TSE+0x19ca:

fffff800`44b119ca 81e1010100ff    and     ecx,0FF000101h

fffff800`44b119d0 66897d00        mov     word ptr [rbp],di

fffff800`44b119d4 81c901010000    or      ecx,101h

fffff800`44b119da 41b849545345    mov     r8d,45535449h

fffff800`44b119e0 894d02          mov     dword ptr [rbp+2],ecx

fffff800`44b119e3 418bd6          mov     edx,r14d

fffff800`44b119e6 b900010000      mov     ecx,100h

fffff800`44b119eb ff15ef760000    call    qword ptr [TSE+0x90e0 (fffff800`44b190e0)]

**From WDM.H:**  
**#define POOL\_FLAG\_PAGED         0x0000000000000100UI64     // Paged pool**

<https://hsdes.intel.com/appstore/article/#/14020226408>

[LNL][PSE] System fail to reboot or cold boot with Microsoft Pluton HECI driver and its pairing RT FW:

When Pluton HECI driver starts PoFx device power management, all device’s components automatically go into Idle condition, unless the driver retains an Active reference.

In this case, the driver has started device power management and has received component Idle condition callback, but has not completed it by calling PoFxCompleteIdleCondition API as required (<https://learn.microsoft.com/en-us/windows-hardware/drivers/ddi/wdm/nc-wdm-po_fx_component_idle_condition_callback>). This stalls PoFx state machine and when PnP Manager tries to Activate device, the Default PEP Activation activity cannot proceed because component has not finished idling yet. Since PnP Manager blocks, it holds the PnP Engine lock and Device Tree lock and this blocks Power Manager’s operations which results in Bugcheck 9F - DRIVER\_POWER\_STATE\_FAILURE (see attached memory dump):

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

**DRIVER\_POWER\_STATE\_FAILURE (9f)**

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

**Arguments:**

**Arg1: 0000000000000004, The power transition timed out waiting to synchronize with the Pnp**

**subsystem.**

**Arg2: 000000000000012c, Timeout in seconds.**

**Arg3: ffffcf8820983040, The thread currently holding on to the Pnp lock.**

**Arg4: ffffce872446f690, nt!TRIAGE\_9F\_PNP on Win7 and higher**

**2: kd> .thread /p /r ffffcf8820983040**

**Implicit thread is now ffffcf88`20983040**

**Implicit process is now ffffcf88`208e9040**

**Loading User Symbols**

**2: kd> kn**

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

**# Child-SP          RetAddr               Call Site**

**00 ffffce87`244f2330 fffff801`13c88055     nt!KiSwapContext+0x76**

**01 ffffce87`244f2470 fffff801`13c89b27     nt!KiSwapThread+0x11f5**

**02 ffffce87`244f25b0 fffff801`13c8cca4     nt!KiCommitThreadWait+0x147**

**03 ffffce87`244f2650 fffff801`13dd6b4f     nt!KeWaitForSingleObject+0x2b4**

**04 ffffce87`244f2740 fffff801`13dd6a02     nt!PopFxActivateDevice+0x13f**

**05 ffffce87`244f27a0 fffff801`1428086d     nt!PoFxActivateDevice+0xe**

**06 ffffce87`244f27d0 fffff801`141c773d     nt!PiProcessQueryDeviceState+0x3d**

**07 ffffce87`244f2840 fffff801`13d4beb3     nt!PiProcessRequeryDeviceState+0x69**

**08 ffffce87`244f2880 fffff801`13d5e445     nt!PnpDeviceActionWorker+0x513**

**09 ffffce87`244f2950 fffff801`13dc1177     nt!ExpWorkerThread+0x155**

**0a ffffce87`244f2b30 fffff801`13e8d4f4     nt!PspSystemThreadStartup+0x57**

**0b ffffce87`244f2b80 00000000`00000000     nt!KiStartSystemThread+0x34**

**2: kd> .frame /r 6**

**06 ffffce87`244f27d0 fffff801`141c773d     nt!PiProcessQueryDeviceState+0x3d**

**rax=0000000000000000 rbx=ffffcf88237d3be0 rcx=0000000000000000**

**rdx=0000000000000000 rsi=0000000000000000 rdi=ffffcf88237d3be0**

**rip=fffff8011428086d rsp=ffffce87244f27d0 rbp=ffffce87244f28e9**

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

**r11=0000000000000000 r12=0000000000000000 r13=ffffffffffffffff**

**r14=ffffcf8821ecc360 r15=0000000000000001**

**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!PiProcessQueryDeviceState+0x3d:**

**fffff801`1428086d 0fbaabc002000008 bts     dword ptr [rbx+2C0h],8 ds:ffffcf88`237d3ea0=00021000**

**2: kd> ub**

**nt!PiProcessQueryDeviceState+0x17:**

**fffff801`14280847 4c8bf1          mov     r14,rcx**

**fffff801`1428084a 4883601000      and     qword ptr [rax+10h],0**

**fffff801`1428084f 488b8138010000  mov     rax,qword ptr [rcx+138h]**

**fffff801`14280856 488d4c2478      lea     rcx,[rsp+78h]**

**fffff801`1428085b 488b5828        mov     rbx,qword ptr [rax+28h]**

**fffff801`1428085f e8e08ee8ff      call    nt!PiPnpRtlBeginOperation (fffff801`14109744)**

**fffff801`14280864 488b4b20        mov     rcx,qword ptr [rbx+20h]**

**fffff801`14280868 e88761b5ff      call    nt!PoFxActivateDevice (fffff801`13dd69f4)**

**2: kd> !devstack poi(ffffcf88237d3be0+20)**

**!DevObj           !DrvObj            !DevExt           ObjectName**

**ffffcf882aacade0  \Driver\PlutonHeci ffffcf882b457fa0**

**> ffffcf8821ecc360  \Driver\pci        ffffcf8821ecc4b0  NTPNP\_PCI0013**

**!DevNode ffffcf88237d3be0 :**

**DeviceInst is "PCI\VEN\_8086&DEV\_A862&SUBSYS\_72708086&REV\_00\3&11583659&0&98"**

**ServiceName is "PlutonHeci"**

**2: kd> dt nt!\_DEVICE\_NODE ffffcf88237d3be0 FxDevice**

**+0x050 FxDevice : 0xffffcf88`2a977980 \_POP\_FX\_DEVICE**

**2: kd> dt 0xffffcf88`2a977980 \_POP\_FX\_DEVICE Components**

**nt!\_POP\_FX\_DEVICE**

**+0x368 Components : 0xffffcf88`2ab89010  -> 0xffffcf88`2ab89018 \_POP\_FX\_COMPONENT**

**2: kd> dt  0xffffcf88`2ab89018 \_POP\_FX\_COMPONENT IdleConditionComplete**

**nt!\_POP\_FX\_COMPONENT**

**+0x088 IdleConditionComplete : 0n1**

**2: kd> !fxdevice -v 0xffffcf88`2a977980**

**!fxdevice 0xffffcf882a977980**

**Device Object: 0xffffcf8821ecc360**

**DevNode: 0xffffcf88237d3be0**

**UniqueId: "PCI\VEN\_8086&DEV\_A862&SUBSYS\_72708086&REV\_00\3&11583659&0&98"**

**InstancePath: "PCI\VEN\_8086&DEV\_A862&SUBSYS\_72708086&REV\_00\3&11583659&0&98"**

**Device Power State: PowerDeviceD0**

**PEP Owner: Default PEP**

**Acpi Plugin: 0**

**Acpi Handle: 0**

**Device Status Flags: DevicePowerRequired**

**Device Idle Timeout: 0000000000**

**Device Power On: No Activity**

**Device Power Off: No Activity**

**Device Unregister: No Activity**

**Component Count: 1**

**Component 0: Current:F0/Deepest:F3 - IDLING (RefCount = 1)**

**Pep Component: 0xffffcf8828b620d0**

**Active: 0  Latency: 3 Residency: 3    Wake: 3     Dx IRP: 3  WW IRP: 3**

**Component Idle State Change: No Activity**

**Component Activation: No Activity**

**Component Active: Running**

**Log has 5 entries starting at 0:**

**#      IntTime       CPU   Cid   Tid**

**---  ----------------  ----  ----  ----**

**0  00000000aa3b6807     0     4   264  Device registered with 1 component(s)**

**1  00000000aa3b6807     0     4   264  Start power management**

**2  00000000aa3b6807     0     4   264  Component 0 latency set to 8000001**

**3  00000000aa3b6807     0     4   264  Component 0 residency set to 120000001**

**4  00000000aa3bb618     1     4   268  Driver component 0 idle condition callback pending**

<https://hsdes.intel.com/appstore/article/#/22018753558>

[MUST-FIX] Dell JIT-266738 - R740 | Intel X710/i350 rNDC with SET Teaming encounters BSOD with VMQ enabled.:

VmsVmqPvtGetScalerTypeForMemberAdapter attempts to dereference NULL-pointer because NicExt MemberAdapterWrapper is NULL:

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

**SYSTEM\_SERVICE\_EXCEPTION (3b)**

**An exception happened while executing a system service routine.**

**Arguments:**

**Arg1: 00000000c0000005, Exception code that caused the BugCheck**

**Arg2: fffff80ff9d118a3, Address of the instruction which caused the BugCheck**

**Arg3: fffffc0077c6dfc0, Address of the context record for the exception that caused the BugCheck**

**Arg4: 0000000000000000, zero.**

**0: kd> r cr2**

**cr2=0000000000000fbd**

**0: kd> u fffff80ff9d118a3 L1**

**vmswitch!VmsVmqPvtGetScalerTypeForMemberAdapter+0xd [inlined in vmswitch!VmsVmqPvtAllocateVmq+0xc73]:**

**fffff80f`f9d118a3 3882bd0f0000    cmp     byte ptr [rdx+0FBDh],al**

**0: kd> k**

**# Child-SP          RetAddr               Call Site**

**00 fffffc00`77c6d688 fffff806`09443a69     nt!KeBugCheckEx**

**01 fffffc00`77c6d690 fffff806`09442bbc     nt!KiBugCheckDispatch+0x69**

**02 fffffc00`77c6d7d0 fffff806`0943995f     nt!KiSystemServiceHandler+0x7c**

**03 fffffc00`77c6d810 fffff806`09283291     nt!RtlpExecuteHandlerForException+0xf**

**04 fffffc00`77c6d840 fffff806`09287894     nt!RtlDispatchException+0x301**

**05 fffffc00`77c6df90 fffff806`09443b8e     nt!KiDispatchException+0x304**

**06 fffffc00`77c6e670 fffff806`0943f226     nt!KiExceptionDispatch+0x10e**

**07 fffffc00`77c6e850 fffff80f`f9d118a3     nt!KiPageFault+0x426**

**08 (Inline Function) --------`--------     vmswitch!VmsVmqPvtGetScalerTypeForMemberAdapter+0xd**

**09 fffffc00`77c6e9e0 fffff80f`f9c386e1     vmswitch!VmsVmqPvtAllocateVmq+0xc73**

**0a fffffc00`77c6eaa0 fffff80f`f9c383de     vmswitch!VmsVmqPvtAllocateVmqAndPropagateChanges+0x161**

**0b fffffc00`77c6eb00 fffff80f`f9c379d3     vmswitch!VmsVmqPvtAllocateVmqForNic+0xea**

**0c fffffc00`77c6eb60 fffff80f`f9cd51bd     vmswitch!VmsVmqDoVmqOperation+0x1eb**

**0d fffffc00`77c6ebd0 fffff80f`f9c86612     vmswitch!VmsOmNicConnect+0x1cd9**

**0e fffffc00`77c6eda0 fffff80f`f9c4c56e     vmswitch!VmsCdpNicConnect+0x67a**

**0f fffffc00`77c6eef0 fffff806`0b43240d     vmswitch!VmsCdpDeviceControl+0x59a9e**

**10 fffffc00`77c6efd0 fffff806`093b6397     VmsProxy!VmsProxyDeviceControl+0xad**

**11 fffffc00`77c6f020 fffff806`09a69468     nt!IopfCallDriver+0x53**

**12 fffffc00`77c6f060 fffff806`09456e55     nt!IovCallDriver+0x264**

**13 fffffc00`77c6f0a0 fffff806`0971050e     nt!IofCallDriver+0x143cb5**

**14 (Inline Function) --------`--------     nt!IoCallDriverWithTracing+0x58**

**15 (Inline Function) --------`--------     nt!IopCallDriverReference+0x150**

**16 fffffc00`77c6f0e0 fffff806`0967af6d     nt!IopSynchronousServiceTail+0x33e**

**17 fffffc00`77c6f180 fffff806`0967b026     nt!IopXxxControlFile+0xc7d**

**18 fffffc00`77c6f2c0 fffff806`09443185     nt!NtDeviceIoControlFile+0x56**

**19 fffffc00`77c6f330 00007ffa`9575f554     nt!KiSystemServiceCopyEnd+0x25**

**1a 000000ce`1effdca8 00000000`00000000     0x00007ffa`9575f554**

**0: kd> .frame /r 9**

**09 fffffc00`77c6e9e0 fffff80f`f9c386e1     vmswitch!VmsVmqPvtAllocateVmq+0xc73**

**rax=0000000000000000 rbx=0000000000000001 rcx=fffff80ff9dafe90**

**rdx=0000000000000000 rsi=ffffd88283b9b000 rdi=ffffd8832f112ed0**

**rip=fffff80ff9d118a3 rsp=fffffc0077c6e9e0 rbp=fffffc0077c6ea58**

**r8=0000000000000000  r9=ffffd8826ea4c1c0 r10=0000000000000000**

**r11=fffffc0077c6e9d0 r12=0000000000000001 r13=0000000000000000**

**r14=0000000000000000 r15=ffffd8832d119000**

**iopl=0         nv up ei ng nz na po nc**

**cs=0010  ss=0018  ds=002b  es=002b  fs=0053  gs=002b             efl=00040286**

**vmswitch!VmsVmqPvtAllocateVmq+0xc73:**

**fffff80f`f9d118a3 3882bd0f0000    cmp     byte ptr [rdx+0FBDh],al ds:002b:00000000`00000fbd=??**

**0: kd> ub**

**vmswitch!VmsVmqPvtAllocateVmq+0xc55:**

**fffff80f`f9d11885 488b4de8        mov     rcx,qword ptr [rbp-18h]**

**fffff80f`f9d11889 448bf0          mov     r14d,eax**

**fffff80f`f9d1188c 44886558        mov     byte ptr [rbp+58h],r12b**

**fffff80f`f9d11890 8b998c010000    mov     ebx,dword ptr [rcx+18Ch]**

**fffff80f`f9d11896 488b55d8        mov     rdx,qword ptr [rbp-28h]**

**fffff80f`f9d1189a 33c0            xor     eax,eax**

**fffff80f`f9d1189c 895dd4          mov     dword ptr [rbp-2Ch],ebx**

**fffff80f`f9d1189f 448975d0        mov     dword ptr [rbp-30h],r14d**

**0: kd> dq fffffc0077c6ea58-28 L1**

**fffffc00`77c6ea30  00000000`00000000**

**0: kd> u fffff80f`f9d114cf L2**

**vmswitch!VmsVmqPvtAllocateVmq+0x89f:**

**fffff80f`f9d114cf 488b86900c0000  mov     rax,qword ptr [rsi+0C90h]**

**fffff80f`f9d114d6 488945d8        mov     qword ptr [rbp-28h],rax**

**0: kd> dt    ptNicExt MemberAdapterWrapper**

**Local var @ rsi Type \_VMS\_PROTOCOL\_EXT\***

**+0xc90 MemberAdapterWrapper : (null)**

<https://hsdes.intel.com/appstore/article/#/18032675835>

[Fe][Sev2 CRI-AKS ICM]:BSOD (DRIVER IRQL NOT LESS OR EQUAL ) observed after enabling driver verifier (a) During S4 cycle.:

This issue is not caused by Intel components, it is caused by the interaction between Ancillary Function Driver for WinSock (AFD.SYS) and AF\_UNIX socket provider (afunix.sys), see attached memory dump.

This is Bugcheck DRIVER\_IRQL\_NOT\_LESS\_OR\_EQUAL (d1):

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

**DRIVER\_IRQL\_NOT\_LESS\_OR\_EQUAL (d1)**

**An attempt was made to access a pageable (or completely invalid) address at an**

**interrupt request level (IRQL) that is too high.  This is usually**

**caused by drivers using improper addresses.**

**If kernel debugger is available get stack backtrace.**

**Arguments:**

**Arg1: ffff8a8ed3a1efb8, memory referenced**

**Arg2: 0000000000000002, IRQL**

**Arg3: 0000000000000000, value 0 = read operation, 1 = write operation**

**Arg4: fffff809f3a1e135, address which referenced memory**

The afd!AfdBCommonChainedReceiveEventHandler attempted to read from virtual address ffff8a8ed3a1efb8:

3: kd> u fffff809f3a1e135 L1

afd!AfdBCommonChainedReceiveEventHandler+0x375:

fffff809`f3a1e135 488b4608        mov     rax,qword ptr [rsi+8]

3: kd> r cr2

cr2=ffff8a8ed3a1efb8

The address is not valid as the page has been paged out:

3: kd> !pte ffff8a8ed3a1efb8

                                           VA ffff8a8ed3a1efb8

PXE at FFFFF379BCDE68A8    PPE at FFFFF379BCD151D8    PDE at FFFFF379A2A3B4E8    PTE at FFFFF3454769D0F0

contains 0A000008AA71C863  contains 0A0000013D239863  contains 3A000006A3BC5863  contains 00000006A27A0880

pfn 8aa71c    ---DA--KWEV  pfn 13d239    ---DA--KWEV  pfn 6a3bc5    ---DA--KWEV  not valid

                                                                                  Transition: 6a27a0

                                                                                  Protect: 4 - ReadWrite

From the Driver Verifier’s log, we can see afunix!AfUnixDeliverEndpointQueueSendRequest has allocated the memory:

3: kd> !verifier 80 ffff8a8ed3a1efb8 1

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 0xffff8a8ed3a1efb8.

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

Pool block ffff8a8ed3a1efb0, Size 0000000000000048, Thread ffffcf8aa2960080

fffff8022509ba3b nt!VfHandlePoolAlloc+0x3db

fffff80224c11358 nt!DifExAllocatePool2Wrapper+0x128

fffff8022509b191 nt!VerifierExAllocatePool2+0x101

fffff809f39f9d5b afunix!AfUnixDeliverEndpointQueueSendRequest+0x27

fffff809f39f9f3e afunix!AfUnixDeliverEndpointSend+0x14a

fffff809f39f1285 afunix!AfUnixTlConnectEndpointSend+0x115

fffff809f3a1dc21 afd!AfdTLStartBufferedVcSend+0xc9

fffff809f3a1d9d5 afd!AfdFastConnectionSend+0x3d5

fffff809f3a1a368 afd!AfdFastIoDeviceControl+0xb98

fffff80224ca515a nt!IopXxxControlFile+0x38a

fffff80224ca4db6 nt!NtDeviceIoControlFile+0x56

fffff80224a33075 nt!KiSystemServiceCopyEnd+0x25

Parsed 000000000000000d entries out of 0000000000020000.

Disassembling the afunix!AfUnixDeliverEndpointQueueSendRequest, we can see it allocates the memory as PAGED\_POOL:

<https://learn.microsoft.com/en-us/windows-hardware/drivers/ddi/wdm/nf-wdm-exallocatepool2>

3: kd> u afunix!AfUnixDeliverEndpointQueueSendRequest afunix!AfUnixDeliverEndpointQueueSendRequest+0x27

afunix!AfUnixDeliverEndpointQueueSendRequest:

fffff809`f39f9d34 48895c2408      mov     qword ptr [rsp+8],rbx

fffff809`f39f9d39 57              push    rdi

fffff809`f39f9d3a 4883ec20        sub     rsp,20h

fffff809`f39f9d3e 488bfa          mov     rdi,rdx

fffff809`f39f9d41 488bd9          mov     rbx,rcx

fffff809`f39f9d44 ba48000000      mov     edx,48h

fffff809`f39f9d49 b900010000      mov     ecx,100h    ; ç POOL\_FLAG\_PAGED                    <https://learn.microsoft.com/en-us/windows-hardware/drivers/kernel/pool_flags>

fffff809`f39f9d4e 41b8576e7069    mov     r8d,69706E57h

fffff809`f39f9d54 48ff15e5d2ffff  call    qword ptr [afunix!\_imp\_ExAllocatePool2 (fffff809`f39f7040)]

fffff809`f39f9d5b 0f1f440000      nop     dword ptr [rax+rax]

But afd!AfdBCommonChainedReceiveEventHandler acquires a Spin Lock:

3: kd> u fffff809`f3a1dea8 L1

afd!AfdBCommonChainedReceiveEventHandler+0xe8:

fffff809`f3a1dea8 48ff1501fa0400  call    qword ptr [afd!\_imp\_KeAcquireInStackQueuedSpinLock (fffff809`f3a6d8b0)]

And this raises the IRQL to DISPATCH\_LEVEL:

3: kd> !irql

Debugger saved IRQL for processor 0x3 -- 2 (DISPATCH\_LEVEL)

“The DRIVER\_IRQL\_NOT\_LESS\_OR\_EQUAL bug check has a value of 0x000000D1. This indicates that a kernel-mode driver attempted to access pageable memory while the process IRQL that was too high.”

<https://learn.microsoft.com/en-us/windows-hardware/drivers/debugger/bug-check-0xd1--driver-irql-not-less-or-equal>

The IRQL is too high, because afd!AfdBCommonChainedReceiveEventHandler has acquired a Spin Lock.  
The memory is PAGEABLE because afunix!AfUnixDeliverEndpointQueueSendRequest allocated it as such.  
Therefore, the issue is caused by the interaction between AFD.SYS and AFUNIX.SYS – one is elevating the IRQL and another one is supplying PAGEABLE memory.

There is no evidence of any kind nor any analysis provided to indicate that this issue is caused by any Intel component or ingredient.

It looks like this issue is fixed already as in newer OS builds, afunix!AfUnixDeliverEndpointQueueSendRequest allocates memory as non-Paged.

<https://hsdes.intel.com/appstore/article/#/14019989146>

[MTL-P][682][C0][DPMT] BSOD: IRQL\_NOT\_LESS\_OR\_EQUAL (a) pointing to BSOD\_MOD\_nt while running Concurrency stress in Core/Uncore(Threadrunner) + Memory(Threadrunner, Lamt) + PSF(FIO)\_DPMT\_:

You have a #PF exception generated for a valid virtual address - this indicates processor our-of-spec behavior.

Page faults should must not occur on stores to a valid VA.

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

**IRQL\_NOT\_LESS\_OR\_EQUAL (a)**

**An attempt was made to access a pageable (or completely invalid) address at an**

**interrupt request level (IRQL) that is too high.  This is usually**

**caused by drivers using improper addresses.**

**If a kernel debugger is available get the stack backtrace.**

**Arguments:**

**Arg1: ffff820356a821d0, memory referenced**

**Arg2: 0000000000000002, IRQL**

**Arg3: 0000000000000001, bitfield :**

**bit 0 : value 0 = read operation, 1 = write operation**

**bit 3 : value 0 = not an execute operation, 1 = execute operation (only on chips which support this level of status)**

**Arg4: fffff8004831807f, address which referenced memory**

**15: kd> r cr2**

**cr2=ffff820356a821d0**

**15: kd> k**

**# Child-SP          RetAddr               Call Site**

**00 ffffa204`21e56e98 fffff800`484417a9     nt!KeBugCheckEx**

**01 ffffa204`21e56ea0 fffff800`4843ce34     nt!KiBugCheckDispatch+0x69**

**02 ffffa204`21e56fe0 fffff800`4831807f     nt!KiPageFault+0x474**

**03 ffffa204`21e57170 fffff800`4823d7eb     nt!KiAcquireKobjectLockSafe+0xf**

**04 ffffa204`21e571a0 fffff800`485b7df2     nt!KeSetEvent+0x6b**

**05 ffffa204`21e57230 fffff800`48338673     nt!PsDispatchIumService+0x96e**

**06 ffffa204`21e574a0 fffff800`489589d7     nt!VslpEnterIumSecureMode+0x287**

**07 ffffa204`21e57570 fffff800`485893b1     nt!VslRundownSecureProcess+0x47**

**08 ffffa204`21e57620 fffff800`488b4315     nt!KeRundownSecureProcess+0x15**

**09 ffffa204`21e57650 fffff800`486f15ca     nt!PspRundownSingleProcess+0x224e41**

**0a ffffa204`21e576e0 fffff800`486f2898     nt!PspExitThread+0x64e**

**0b ffffa204`21e577e0 fffff800`482ce76d     nt!KiSchedulerApcTerminate+0x38**

**0c ffffa204`21e57820 fffff800`48432290     nt!KiDeliverApc+0x47d**

**0d ffffa204`21e578e0 fffff800`48440f8f     nt!KiInitiateUserApc+0x70**

**0e ffffa204`21e57a20 00007ff9`adc6ecd4     nt!KiSystemServiceExit+0x9f**

**0f 00000008`b7fff348 00000000`00000000     0x00007ff9`adc6ecd4**

**15: kd> !pte ffff820356a821d0**

**VA ffff820356a821d0**

**PXE at FFFFECF67B3D9820    PPE at FFFFECF67B304068    PDE at FFFFECF66080D5A8    PTE at FFFFECC101AB5410**

**contains 0A00000374A00863  contains 0A00000374A01863  contains 0A0000036D16D863  contains 87000002A300D921**

**pfn 374a00    ---DA--KWEV  pfn 374a01    ---DA--KWEV  pfn 36d16d    ---DA--KWEV  pfn 2a300d    -G--A--KR-V**

**15: kd> !pool ffff820356a821d0**

**Pool page ffff820356a821d0 region is Paged pool**

**ffff820356a82030 size:   a0 previous size:    0  (Free)       Wnf**

**ffff820356a820d0 size:   a0 previous size:    0  (Allocated)  Wnf**

**\*ffff820356a82170 size:   a0 previous size:    0  (Allocated) \*PsVe Process: ffffd98fd4ce3140**

**Owning component : Unknown (update pooltag.txt)**

**ffff820356a82210 size:   a0 previous size:    0  (Free)       Sect**

**ffff820356a822b0 size:   a0 previous size:    0  (Free)       Sect**

**ffff820356a82350 size:   a0 previous size:    0  (Free)       Wnf**

**ffff820356a823f0 size:   a0 previous size:    0  (Free)       Sect**

**ffff820356a82490 size:   a0 previous size:    0  (Allocated)  SeAt**

**ffff820356a82530 size:   a0 previous size:    0  (Allocated)  Wnf  Process: ffffd98fd4e1c0c0**

**ffff820356a825d0 size:   a0 previous size:    0  (Allocated)  Wnf  Process: ffffd98fd4418080**

**ffff820356a82670 size:   a0 previous size:    0  (Free)       Sect**

**ffff820356a82710 size:   a0 previous size:    0  (Allocated)  Ntfc**

**ffff820356a827b0 size:   a0 previous size:    0  (Free)       Sect**

**ffff820356a82850 size:   a0 previous size:    0  (Free)       Sect**

**ffff820356a828f0 size:   a0 previous size:    0  (Allocated)  Ntfc**

**ffff820356a82990 size:   a0 previous size:    0  (Allocated)  Sect**

**ffff820356a82a30 size:   a0 previous size:    0  (Allocated)  Ntfc**

**ffff820356a82ad0 size:   a0 previous size:    0  (Free)       AlVi**

**ffff820356a82b70 size:   a0 previous size:    0  (Allocated)  Sect**

**ffff820356a82c10 size:   a0 previous size:    0  (Allocated)  SeAt**

**ffff820356a82cb0 size:   a0 previous size:    0  (Allocated)  Ntfc**

**ffff820356a82d50 size:   a0 previous size:    0  (Free)       Sect**

**ffff820356a82df0 size:   a0 previous size:    0  (Allocated)  Sect**

**ffff820356a82e90 size:   a0 previous size:    0  (Allocated)  Sect**

**ffff820356a82f30 size:   a0 previous size:    0  (Free)       Ntfc**

I suggest to refer this issue to Silicon Validation, given that this is MTL 682 which has multiple "strange" HW behaviors.

<https://hsdes.intel.com/appstore/article/#/22018599595>

[MTL-P][C0][Concurrency][CORP][DC5] Observed BSOD: SYSTEM\_THREAD\_EXCEPTION\_NOT\_HANDLED pointing to dxgkrnl race condition while running P95\_CPU10\_12\_LargeFFT\_3DMark\_Idle.json:

**Summary:**

**This is a race condition in DXGK** - component relations cannot be removed as surprise removal IRP has been processed because Fx device is already unregistered.

This issue is similar to  <https://hsdes.intel.com/appstore/article/#/16014251703> and was promoted MSFT, but there was no fix from MSFT.

We have 4 dumps hence this is high priority issue to be investigated/Fixed by Microsoft.

**Debug details:**

1: 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: fffff80172fa0589, The address that the exception occurred at

Arg3: ffffad0bf378f208, Exception Record Address

Arg4: ffffad0bf378ea20, Context Record Address

1: kd> u fffff80172fa0589 L1  
nt!PoFxRemoveComponentRelation+0x59   
fffff801`72fa0589 488b04c8        mov     rax,qword ptr [rax+rcx\*8]

1: kd> k

 # Child-SP          RetAddr               Call Site

00 ffffad0b`f378e198 fffff801`72e4baf3     nt!KeBugCheckEx

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

02 ffffad0b`f378e1a0 fffff801`72ded661     nt!PspSystemThreadStartup$filt$0+0x44

03 ffffad0b`f378e1e0 fffff801`72e3735f     nt!\_\_C\_specific\_handler+0xa1

04 ffffad0b`f378e250 fffff801`72c4da03     nt!RtlpExecuteHandlerForException+0xf

05 ffffad0b`f378e280 fffff801`72ccf15e     nt!RtlDispatchException+0x2f3

06 ffffad0b`f378e9f0 fffff801`72e418fc     nt!KiDispatchException+0x1ae

07 ffffad0b`f378f0d0 fffff801`72e3ce0e     nt!KiExceptionDispatch+0x13c

08 ffffad0b`f378f2b0 fffff801`72fa0589     nt!KiPageFault+0x44e

09 ffffad0b`f378f440 fffff801`8b03958b     nt!PoFxRemoveComponentRelation+0x59

0a ffffad0b`f378f4b0 fffff801`8b039080     dxgkrnl!DxgMonitor::Usb4HostRouterPoFxRef::RemoveUsb4HRPowerRef+0x43

0b (Inline Function) --------`--------     dxgkrnl!DxgMonitor::Usb4HostRouterPoFxRef::OnCleanup+0x9

0c ffffad0b`f378f530 fffff801`8b038740     dxgkrnl!DxgMonitor::MonitorUsb4State::DestroyPowerConnectionWithUsb4Stack+0x2c

0d ffffad0b`f378f560 fffff801`8b03795a     dxgkrnl!DxgMonitor::MonitorUsb4State::~MonitorUsb4State+0x10

0e ffffad0b`f378f590 fffff801`8acacc64     dxgkrnl!DXGMONITOR::~DXGMONITOR+0xce

0f ffffad0b`f378f5e0 fffff801`8ae9c6fa     dxgkrnl!DXGMONITOR::`scalar deleting destructor'+0x14

10 ffffad0b`f378f610 fffff801`8b035d39     dxgkrnl!MONITOR\_MGR::\_DestroyPhysicalMonitor+0xb2

11 ffffad0b`f378f650 fffff801`8aced654     dxgkrnl!MONITOR\_MGR::~MONITOR\_MGR+0x115

12 ffffad0b`f378f6e0 fffff801`8af26a6e     dxgkrnl!MONITOR\_MGR::`scalar deleting destructor'+0x14

13 (Inline Function) --------`--------     dxgkrnl!MonitorDestroyMonitorManager+0x23

14 ffffad0b`f378f710 fffff801`8af20e41     dxgkrnl!ADAPTER\_DISPLAY::Destroy+0x252

15 ffffad0b`f378f780 fffff801`8af25037     dxgkrnl!DXGADAPTER::Destroy+0x9d

16 ffffad0b`f378f8b0 fffff801`8af1beda     dxgkrnl!DXGADAPTER::Stop+0x4cb

17 (Inline Function) --------`--------     dxgkrnl!DxgkRemoveAdapter+0x3a

18 ffffad0b`f378fa10 fffff801`72cccfd7     dxgkrnl!DpiPowerArbiterThread+0x9038a

19 ffffad0b`f378fb30 fffff801`72e31054     nt!PspSystemThreadStartup+0x57

1a ffffad0b`f378fb80 00000000`00000000     nt!KiStartSystemThread+0x34

1: kd> .frame /r a

0a ffffad0b`f378f4b0 fffff801`8b039080     dxgkrnl!DxgMonitor::Usb4HostRouterPoFxRef::RemoveUsb4HRPowerRef+0x43

rax=0000000000000000 rbx=ffffd48f63684650 rcx=0000000000000013

rdx=0000000000000013 rsi=ffffad0bf378f670 rdi=ffffd48f63684610

rip=fffff8018b03958b rsp=ffffad0bf378f4b0 rbp=0000000000000000

 r8=ffffd48f457e6dc0  r9=fffff8018ad22508 r10=fffff80172fa0530

r11=0000000000014090 r12=0000000000000201 r13=0000000000000000

r14=0000000000000000 r15=0000000000000000

iopl=0         nv up ei ng nz na po nc

cs=0010  ss=0000  ds=002b  es=002b  fs=0053  gs=002b             efl=00040286

dxgkrnl!DxgMonitor::Usb4HostRouterPoFxRef::RemoveUsb4HRPowerRef+0x43:

fffff801`8b03958b 4863f8          movsxd  rdi,eax

1: kd> dt this \_PoFxHandle

Local var @ rbx Type DxgMonitor::Usb4HostRouterPoFxRef\*

   +0x010 \_PoFxHandle : 0xffffd48f`6371b010 POHANDLE\_\_

1: kd>  dt nt!\_POP\_FX\_DEVICE 0xffffd48f`6371b010 Components

   +0x340 Components : (null)

1: kd>  !pool 0xffffd48f`6371b010

Pool page ffffd48f6371b010 region is Nonpaged pool

 ffffd48f6371b550 size:  290 previous size:    0  (Allocated)  MmCi

 ffffd48f6371b7e0 size:   40 previous size:    0  (Free)       ...[

 ffffd48f6371b830 size:  250 previous size:    0  (Allocated)  ALPC

 ffffd48f6371baa0 size:  4c0 previous size:    0  (Allocated)  MiIo

 ffffd48f6371bf60 size:   80 previous size:    0  (Free)       ...[

1: kd> dt nt!\_POP\_FX\_DEVICE ffffd48f6371b010 DevNode

   +0x030 DevNode : 0xffffd48f`4545fb60 \_DEVICE\_NODE

Device

1: kd>  dt nt!\_DEVICE\_NODE 0xffffd48f`4545fb60 FxDevice

   +0x050 FxDevice : (null)

1: kd> !DevNode ffffd48f4545fb60  
DevNode 0xffffd48f4545fb60 for PDO 0xffffd48f45559360  
  Parent 0xffffd48f410b78a0   Sibling 0xffffd48f4555fae0   Child 0xffffd48f5f763c40    
  InstancePath is "**PCI\VEN\_8086&DEV\_7D55&SUBSYS\_22128086&REV\_08\3&11583659&0&10**"  
  ServiceName is "igfxn"  
  State = DeviceNodeStarted (0x30a)*@ 2023 Jun 23 16:54:01.137*  Previous State = DeviceNodeStarted (0x30a)*@ 2023 Jun 23 16:53:11.846*  StateHistory[14] = DeviceNodeAwaitingQueuedRemoval (0x311)  
  StateHistory[13] = DeviceNodeStarted (0x30a)  
  StateHistory[12] = DeviceNodeEnumerateCompletion (0x30f)  
  StateHistory[11] = DeviceNodeEnumeratePending (0x30e)  
  StateHistory[10] = DeviceNodeStarted (0x30a)  
  StateHistory[09] = DeviceNodeEnumerateCompletion (0x30f)  
  StateHistory[08] = DeviceNodeEnumeratePending (0x30e)  
  StateHistory[07] = DeviceNodeStarted (0x30a)  
  StateHistory[06] = DeviceNodeEnumerateCompletion (0x30f)  
  StateHistory[05] = DeviceNodeEnumeratePending (0x30e)  
  StateHistory[04] = DeviceNodeStarted (0x30a)  
  StateHistory[03] = DeviceNodeEnumerateCompletion (0x30f)  
  StateHistory[02] = DeviceNodeEnumeratePending (0x30e)  
  StateHistory[01] = DeviceNodeStarted (0x30a)  
  StateHistory[00] = DeviceNodeEnumerateCompletion (0x30f)  
  StateHistory[19] = DeviceNodeEnumeratePending (0x30e)  
  StateHistory[18] = DeviceNodeStarted (0x30a)  
  StateHistory[17] = DeviceNodeEnumerateCompletion (0x30f)  
  StateHistory[16] = DeviceNodeEnumeratePending (0x30e)  
  StateHistory[15] = DeviceNodeStarted (0x30a)  
  Flags (0x6c0000f0)  DNF\_ENUMERATED, DNF\_IDS\_QUERIED,  
                      DNF\_HAS\_BOOT\_CONFIG, DNF\_BOOT\_CONFIG\_RESERVED,  
                      DNF\_NO\_LOWER\_DEVICE\_FILTERS, DNF\_NO\_LOWER\_CLASS\_FILTERS,  
                      DNF\_NO\_UPPER\_DEVICE\_FILTERS, DNF\_NO\_UPPER\_CLASS\_FILTERS  
  CapabilityFlags (0x00400000)   
                                Unknown flags 0x00400000

!poaction

Dumping device event thread...

THREAD ffffe489a0367040  Cid 0004.7434  Teb: 0000000000000000 Win32Thread: 0000000000000000 WAIT: (Executive) KernelMode Non-Alertable

    fffff5889ebdf1e0  SynchronizationEvent

IRP List:

    ffffe489a079adb0: (0006,01f0) Flags: 00000000  Mdl: 00000000

Not impersonating

DeviceMap                 ffff98074dc8bd60

Owning Process            ffffe48973ee8040       Image:         System

Attached Process          N/A            Image:         N/A

Wait Start TickCount      5564022        Ticks: 11 (0:00:00:00.171)

Context Switch Count      9595           IdealProcessor: 10

UserTime                  00:00:00.000

KernelTime                00:00:00.343

Win32 Start Address nt!ExpWorkerThread (0xfffff800070b1450)

Stack Init fffff5889ebdfbb0 Current fffff5889ebdea60

Base fffff5889ebe0000 Limit fffff5889ebd9000 Call 0000000000000000

Priority 13 BasePriority 12 PriorityDecrement 0 IoPriority 2 PagePriority 5

Child-SP          RetAddr               : Args to Child                                                           : Call Site

fffff588`9ebdeaa0 fffff800`07039965     : ffffd181`2df5b180 00000000`00000000 ffffe489`73eb6040 ffffd181`2df5b180 : nt!KiSwapContext+0x76

fffff588`9ebdebe0 fffff800`07037c94     : ffffe489`a0367040 ffffe489`00000000 fffff588`9ebdefce 00000000`00000000 : nt!KiSwapThread+0xae5

fffff588`9ebded30 fffff800`07037016     : 00000000`00000000 00000000`00000001 fffff800`00000000 00000000`00000000 : nt!KiCommitThreadWait+0x134

fffff588`9ebdede0 fffff800`0ca4ed36     : 00000000`00000000 00000000`00000000 ffff9807`52005510 ffffe489`9319b180 : nt!KeWaitForSingleObject+0x256

fffff588`9ebdf180 fffff800`0cbf9070     : ffffe489`96621180 ffffe489`a079adb0 ffffe489`a079adb0 00000000`00000000 : dxgkrnl!DpiRequestIoPowerState+0xbe

fffff588`9ebdf220 fffff800`0cbf9533     : ffffe489`96621180 ffffe489`96622060 ffffe489`96622060 ffffe489`92c4f3f0 : dxgkrnl!DpiFdoHandleStopDevice+0x1d0

fffff588`9ebdf320 fffff800`0ca82ec5     : fffff800`06e1d800 ffffe489`96621117 ffffe489`96621030 00000000`00000000 : dxgkrnl!DpiFdoHandleSurpriseRemoval+0x263

fffff588`9ebdf370 fffff800`0c9ffbca     : ffffe489`96621030 ffffe489`a079adb0 fffff588`9ebdf620 00000000`00000000 : dxgkrnl!DpiFdoDispatchPnp+0xd5

fffff588`9ebdf410 fffff800`07092e25     : ffffe489`96621030 fffff800`070f3330 ffffe489`96621030 fffff588`9ebdf604 : dxgkrnl!DpiDispatchPnp+0xea

fffff588`9ebdf530 fffff800`07523004     : ffffe489`96621030 00000000`00000000 fffff588`9ebdf620 ffffe489`a079adb0 : nt!IofCallDriver+0x55

fffff588`9ebdf570 fffff800`0762935c     : 00000000`00000017 ffffe489`79954360 ffffe489`7994ab60 ffffe489`79954360 : nt!IopSynchronousCall+0xf8

fffff588`9ebdf5e0 fffff800`0762704c     : ffff9807`6e6b32f0 00000000`00000000 00000000`00000311 00000000`0000030a : nt!IopRemoveDevice+0x108

fffff588`9ebdf690 fffff800`07628f64     : ffffe489`7994ab60 00000000`00000000 00000000`00000000 ffff9807`68724850 : nt!PnpSurpriseRemoveLockedDeviceNode+0xc4

fffff588`9ebdf6f0 fffff800`07628bf7     : ffffe489`7994ab60 fffff588`9ebdf770 ffffe489`79954360 00000000`00000004 : nt!PnpDeleteLockedDeviceNode+0x88

fffff588`9ebdf730 fffff800`07629e46     : ffffe489`79954360 fffff588`00000002 00000000`00000000 00000000`00000005 : nt!PnpDeleteLockedDeviceNodes+0xd7

fffff588`9ebdf7b0 fffff800`075512dd     : fffff588`9ebdf8f0 ffffe489`7994ab00 ffffe489`ab65f400 ffff9807`00000007 : nt!PnpProcessQueryRemoveAndEject+0x1da

fffff588`9ebdf890 fffff800`07563f70     : ffff9807`6e6b32f0 ffff9807`55775770 ffffe489`73eb2000 00000000`00000000 : nt!PnpProcessTargetDeviceEvent+0x109

fffff588`9ebdf8c0 fffff800`070b15a5     : ffffe489`73eb2010 ffffe489`a0367040 fffff588`9ebdfa40 fffff800`00000000 : nt!PnpDeviceEventWorker+0x2c0

fffff588`9ebdf940 fffff800`070d9907     : ffffe489`a0367040 00000000`0000207e ffffe489`a0367040 fffff800`070b1450 : nt!ExpWorkerThread+0x155

fffff588`9ebdfb30 fffff800`07233bd4     : ffffd181`2e956180 ffffe489`a0367040 fffff800`070d98b0 00000000`00000246 : nt!PspSystemThreadStartup+0x57

fffff588`9ebdfb80 00000000`00000000     : fffff588`9ebe0000 fffff588`9ebd9000 00000000`00000000 00000000`00000000 : nt!KiStartSystemThread+0x34

17: kd> !irp ffffe489a079adb0

Irp is active with 3 stacks 3 is current (= 0xffffe489a079af10)

 No Mdl: No System Buffer: Thread ffffe489a0367040:  Irp stack trace.

     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

>[IRP\_MJ\_PNP(1b), IRP\_MN\_SURPRISE\_REMOVAL(17)]

            0  0 ffffe48996621030 00000000 00000000-00000000

       \Driver\igfxn

Args: 00000000 00000000 00000000 00000000

[OSD-PR]

<https://hsdes.intel.com/appstore/article/#/15013822095>

[CSPV][CSPV\_SH][HP][TGL][TGL\_IPU\_WW24'23][BSOD] - 0x14F\_DAM\_IMAGE\_dam.sys:

It looks like this issue is caused by a slow performing Optane SSD. I suggest to replace the SSD and see if the problem persists.

Axon link:

|  |
| --- |
| <https://axon.intel.com/app/view/f01b7773-a8f7-ea3d-d247-ee0b86471a56> |

6: kd> !analyze -v

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

\*                                                                             \*

\*                        Bugcheck Analysis                                    \*

\*                                                                             \*

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

PDC\_WATCHDOG\_TIMEOUT (14f)

A system component failed to respond within the allocated time period,

preventing the system from exiting connected standby.

Arguments:

Arg1: 0000000000000004, Client ID of the hung component.

Arg2: 0000000000000002, A resiliency client failed to respond.

Arg3: fffff802527fe750, Pointer to the resiliency client (pdc!\_PDC\_RESILIENCY\_CLIENT).

Arg4: ffff810cc3b472e0, Pointer to a pdc!PDC\_14F\_TRIAGE structure.

Debugging Details:

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

BUGCHECK\_CODE:  14f

BUGCHECK\_P1: 4

BUGCHECK\_P2: 2

BUGCHECK\_P3: fffff802527fe750

BUGCHECK\_P4: ffff810cc3b472e0

IMAGE\_NAME:  dam.sys

BLACKBOXACPI: 1 (!blackboxacpi)

BLACKBOXBSD: 1 (!blackboxbsd)

BLACKBOXNTFS: 1 (!blackboxntfs)

BLACKBOXPNP: 1 (!blackboxpnp)

BLACKBOXWINLOGON: 1

PROCESS\_NAME:  System

STACK\_TEXT:

ffff810c`c3b472a8 fffff802`5280ff75     : 00000000`0000014f 00000000`00000004 00000000`00000002 fffff802`527fe750 : nt!KeBugCheckEx

ffff810c`c3b472b0 fffff802`4fc921ff     : ffffc18c`f76aace0 ffffc18c`f76aac00 ffffc18c`00000000 00000000`00000000 : pdc!PdcpResiliencyWatchdog+0x95

ffff810c`c3b47300 fffff802`4fd647a5     : ffffc18d`15c50040 ffffb181`42c4f000 ffffc18d`15c50040 00570059`0050002e : nt!ExpWorkerThread+0x14f

ffff810c`c3b474f0 fffff802`4fe22644     : ffffb181`42c40180 ffffc18d`15c50040 fffff802`4fd64750 005f0052`004f0053 : nt!PspSystemThreadStartup+0x55

ffff810c`c3b47540 00000000`00000000     : ffff810c`c3b48000 ffff810c`c3b41000 00000000`00000000 00000000`00000000 : nt!KiStartSystemThread+0x34

MODULE\_NAME: dam

STACK\_COMMAND:  .thread ; .cxr ; kb

FAILURE\_BUCKET\_ID:  0x14F\_DAM\_IMAGE\_dam.sys

OS\_VERSION:  10.0.22000.1

BUILDLAB\_STR:  co\_release

OSPLATFORM\_TYPE:  x64

OSNAME:  Windows 10

FAILURE\_ID\_HASH:  {71a660da-efa0-43ad-07ec-33220699ba4c}

Followup:     MachineOwner

---------

6: kd> lmvm dam

Browse full module list

start             end                 module name

fffff802`6d750000 fffff802`6d76e000   dam        (deferred)

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

    Image name: dam.sys

    Browse all global symbols  functions  data

    Image was built with /Brepro flag.

    Timestamp:        ACFEE7A0 (This is a reproducible build file hash, not a timestamp)

    CheckSum:         000231CD

    ImageSize:        0001E000

    Translations:     0000.04b0 0000.04e4 0409.04b0 0409.04e4

    Information from resource tables:

6: kd> !analyze -show

PDC\_WATCHDOG\_TIMEOUT (14f)

A system component failed to respond within the allocated time period,

preventing the system from exiting connected standby.

Arguments:

Arg1: 0000000000000004, Client ID of the hung component.

Arg2: 0000000000000002, A resiliency client failed to respond.

Arg3: fffff802527fe750, Pointer to the resiliency client (pdc!\_PDC\_RESILIENCY\_CLIENT).

Arg4: ffff810cc3b472e0, Pointer to a pdc!PDC\_14F\_TRIAGE structure.

6: kd> dt pdc!\_PDC\_14F\_TRIAGE ffff810cc3b472e0

   +0x000 ClientProcess    : (null)

   +0x008 CallbackThread   : 0xffffc18d`d6c5f040 \_ETHREAD

6: kd> .thread /p /r 0xffffc18d`d6c5f040

Implicit thread is now ffffc18d`d6c5f040

Implicit process is now ffffc18c`f76fc040

Loading User Symbols

6: kd> kn

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

 # Child-SP          RetAddr               Call Site

00 ffff810c`b938d690 fffff802`4fc72d87     nt!KiSwapContext+0x76

01 ffff810c`b938d7d0 fffff802`4fd413fa     nt!KiSwapThread+0x3a7

02 ffff810c`b938d8b0 fffff802`4fc1f962     nt!KiInSwapSingleProcess+0x6a

03 ffff810c`b938d8e0 fffff802`500690e3     nt!KiStackAttachProcess+0x352

04 ffff810c`b938d960 fffff802`4fc03869     nt!PspChangeProcessExecutionState+0xef

05 ffff810c`b938da20 fffff802`5014f9fe     nt!PspExecuteJobFreezeThawCallback+0x69

06 ffff810c`b938da70 fffff802`5014f466     nt!PspCallJobHierarchyCallbacks+0xba

07 ffff810c`b938dac0 fffff802`5006e8c1     nt!PspEnumJobsAndProcessesInJobHierarchy+0x1d2

08 ffff810c`b938db40 fffff802`5006db27     nt!PspFreezeJobTree+0x151

09 ffff810c`b938dc20 fffff802`4fe32185     nt!NtSetInformationJobObject+0xf57

0a ffff810c`b938e900 fffff802`4fe22f50     nt!KiSystemServiceCopyEnd+0x25

0b ffff810c`b938ea98 fffff802`6d7606ce     nt!KiServiceLinkage

0c ffff810c`b938eaa0 fffff802`6d761556     dam!DampFreezeSession0Job+0xd6

0d ffff810c`b938eb40 fffff802`6d7779e8     dam!DampPdcResiliencyCallback+0x1c6

0e ffff810c`b938ebf0 fffff802`5280b7c5     KMPDC!PdcpResiliencyClientCallback+0x158

0f ffff810c`b938ef90 fffff802`4fc921ff     pdc!PdcPortMessageWorkerThread+0xf5

10 ffff810c`b938f300 fffff802`4fd647a5     nt!ExpWorkerThread+0x14f

11 ffff810c`b938f4f0 fffff802`4fe22644     nt!PspSystemThreadStartup+0x55

12 ffff810c`b938f540 00000000`00000000     nt!KiStartSystemThread+0x34

6: kd> .frame 0n8;dv /t /v

08 ffff810c`b938db40 fffff802`5006db27     nt!PspFreezeJobTree+0x151

6: kd> !irp

Free build - use !irpfind to scan memory for any active IRPs

6: kd> !poaction

PopAction: fffff80250622820

  State..........: 0 - Idle

  Updates........: 0

  Action.........: None

  Lightest State.: Unspecified

  Flags..........: 10000003 QueryApps|UIAllowed

  Irp minor......: ??

  System State...: Unspecified

  Hiber Context..: 0000000000000000

Allocated power irps (PopIrpList - fffff80250623010)

  IRP: ffffc18dd7a96db0 (wait-wake/S1), PDO: ffffc18d04cea120

  IRP: ffffc18dc1a6fdb0 (wait-wake/S0), PDO: ffffc18daf92eb40

  IRP: ffffc18de3890920 (wait-wake/S3), PDO: ffffc18db606cb00

  IRP: ffffc18dc15e8a20 (wait-wake/S0), PDO: ffffc18db5c52d80

  IRP: ffffc18deacb8010 (wait-wake/S0), PDO: ffffc18d186ec520

  IRP: ffffc18de3bc0aa0 (wait-wake/S0), PDO: ffffc18d156e8e00

  IRP: ffffc18dd6bb7aa0 (wait-wake/S0), PDO: ffffc18d154ee980

  IRP: ffffc18dd6d2daa0 (wait-wake/S0), PDO: ffffc18cf7b2aaf0

  IRP: ffffc18dd70bdd00 (wait-wake/S0), PDO: ffffc18d047e6360

  IRP: ffffc18dd6eccd00 (wait-wake/S0), PDO: ffffc18d047ee360

  IRP: ffffc18deada3d00 (wait-wake/S0), PDO: ffffc18d160e4780

  IRP: ffffc18dd73d59a0 (wait-wake/S4), PDO: ffffc18d084ce190

  IRP: ffffc18de49b4760 (wait-wake/S4), PDO: ffffc18d08bbf0c0

  IRP: ffffc18d0857ea60 (wait-wake/S4), PDO: ffffc18de4946af0

  IRP: ffffc18dd6be9aa0 (wait-wake/S0), PDO: ffffc18de2de6af0

  IRP: ffffc18dd6a87d00 (wait-wake/S0), PDO: ffffc18de6cac060

  IRP: ffffc18de5e7c9e0 (wait-wake/S4), PDO: ffffc18dae22c7c0

  IRP: ffffc18de10deaa0 (wait-wake/S4), PDO: ffffc18de4760af0

  IRP: ffffc18d097b29e0 (wait-wake/S4), PDO: ffffc18dabc650a0

  IRP: ffffc18db0d8a9a0 (wait-wake/S4), PDO: ffffc18d044e4360

  IRP: ffffc18dd83c1010 (wait-wake/S0), PDO: ffffc18d046e4360

  IRP: ffffc18de546e9e0 (wait-wake/S0), PDO: ffffc18de6bb3b30

  IRP: ffffc18dd0a89aa0 (wait-wake/S0), PDO: ffffc18dd71a7af0

  IRP: ffffc18dd0e11d20 (wait-wake/S0), PDO: ffffc18d07e38060

  IRP: ffffc18db1fe2d00 (wait-wake/S0), PDO: ffffc18d07f52060

  IRP: ffffc18dae4a1d00 (wait-wake/S0), PDO: ffffc18d323020a0

  IRP: ffffc18dab57dd00 (wait-wake/S0), PDO: ffffc18d082af060

Irp worker threads (PopIrpThreadList - fffff8025061fb40)

  THREAD: ffffc18cf772c040 (static)

  THREAD: ffffc18cf772d040 (static)

  THREAD: ffffc18ddf908040 (dynamic)

  THREAD: ffffc18ddfb31040 (dynamic)

  THREAD: ffffc18db608e040 (dynamic)

  THREAD: ffffc18de5ca2040 (dynamic)

Broadcast in progress: FALSE

Is Directed DRIPS Transition: FALSE

No Device State present

6: kd> !thread

THREAD ffffc18d15c50040  Cid 0004.bfd4  Teb: 0000000000000000 Win32Thread: 0000000000000000 RUNNING on processor 6

Not impersonating

DeviceMap                 ffffa18e6ee26010

Owning Process            ffffc18cf76fc040       Image:         System

Attached Process          N/A            Image:         N/A

Wait Start TickCount      12110119       Ticks: 12 (0:00:00:00.187)

Context Switch Count      71575          IdealProcessor: 3

UserTime                  00:00:00.000

KernelTime                00:00:02.078

Win32 Start Address nt!ExpWorkerThread (0xfffff8024fc920b0)

Stack Init ffff810cc3b47570 Current ffff810cc3b46f60

Base ffff810cc3b48000 Limit ffff810cc3b41000 Call 0000000000000000

Priority 12 BasePriority 12 PriorityDecrement 0 IoPriority 2 PagePriority 5

Child-SP          RetAddr               : Args to Child                                                           : Call Site

ffff810c`c3b472a8 fffff802`5280ff75     : 00000000`0000014f 00000000`00000004 00000000`00000002 fffff802`527fe750 : nt!KeBugCheckEx

ffff810c`c3b472b0 fffff802`4fc921ff     : ffffc18c`f76aace0 ffffc18c`f76aac00 ffffc18c`00000000 00000000`00000000 : pdc!PdcpResiliencyWatchdog+0x95

ffff810c`c3b47300 fffff802`4fd647a5     : ffffc18d`15c50040 ffffb181`42c4f000 ffffc18d`15c50040 00570059`0050002e : nt!ExpWorkerThread+0x14f

ffff810c`c3b474f0 fffff802`4fe22644     : ffffb181`42c40180 ffffc18d`15c50040 fffff802`4fd64750 005f0052`004f0053 : nt!PspSystemThreadStartup+0x55

ffff810c`c3b47540 00000000`00000000     : ffff810c`c3b48000 ffff810c`c3b41000 00000000`00000000 00000000`00000000 : nt!KiStartSystemThread+0x34

6: kd> lml

start             end                 module name

fffff802`4fa00000 fffff802`50a47000   nt         (pdb symbols)          C:\ProgramData\dbg\sym\ntkrnlmp.pdb\20A9DB03D4E6A9E1ADE642E050E343D61\ntkrnlmp.pdb

fffff802`527f0000 fffff802`5281f000   pdc      # (pdb symbols)          C:\ProgramData\dbg\sym\PDC.pdb\EDC728A52345BEA45A26112E7FFA32531\PDC.pdb

fffff802`6d750000 fffff802`6d76e000   dam        (pdb symbols)          C:\ProgramData\dbg\sym\dam.pdb\1A43343FFB2165A4510347D787B83D2C1\dam.pdb

fffff802`6d770000 fffff802`6d77e000   KMPDC      (pdb symbols)          C:\ProgramData\dbg\sym\KMPDC.pdb\0864C087FC59196994AEDF59023EF9741\KMPDC.pdb

fffff9bf`b6a20000 fffff9bf`b6aca000   win32k   # (pdb symbols)          C:\ProgramData\dbg\sym\win32k.pdb\A88AAF4C1D620E0D434EC67DB042A69F1\win32k.pdb

6: kd> knL

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

 # Child-SP          RetAddr               Call Site

00 ffff810c`b938d690 fffff802`4fc72d87     nt!KiSwapContext+0x76

01 ffff810c`b938d7d0 fffff802`4fd413fa     nt!KiSwapThread+0x3a7

02 ffff810c`b938d8b0 fffff802`4fc1f962     nt!KiInSwapSingleProcess+0x6a

03 ffff810c`b938d8e0 fffff802`500690e3     nt!KiStackAttachProcess+0x352

04 ffff810c`b938d960 fffff802`4fc03869     nt!PspChangeProcessExecutionState+0xef

05 ffff810c`b938da20 fffff802`5014f9fe     nt!PspExecuteJobFreezeThawCallback+0x69

06 ffff810c`b938da70 fffff802`5014f466     nt!PspCallJobHierarchyCallbacks+0xba

07 ffff810c`b938dac0 fffff802`5006e8c1     nt!PspEnumJobsAndProcessesInJobHierarchy+0x1d2

08 ffff810c`b938db40 fffff802`5006db27     nt!PspFreezeJobTree+0x151

09 ffff810c`b938dc20 fffff802`4fe32185     nt!NtSetInformationJobObject+0xf57

0a ffff810c`b938e900 fffff802`4fe22f50     nt!KiSystemServiceCopyEnd+0x25

0b ffff810c`b938ea98 fffff802`6d7606ce     nt!KiServiceLinkage

0c ffff810c`b938eaa0 fffff802`6d761556     dam!DampFreezeSession0Job+0xd6

0d ffff810c`b938eb40 fffff802`6d7779e8     dam!DampPdcResiliencyCallback+0x1c6

0e ffff810c`b938ebf0 fffff802`5280b7c5     KMPDC!PdcpResiliencyClientCallback+0x158

0f ffff810c`b938ef90 fffff802`4fc921ff     pdc!PdcPortMessageWorkerThread+0xf5

10 ffff810c`b938f300 fffff802`4fd647a5     nt!ExpWorkerThread+0x14f

11 ffff810c`b938f4f0 fffff802`4fe22644     nt!PspSystemThreadStartup+0x55

12 ffff810c`b938f540 00000000`00000000     nt!KiStartSystemThread+0x34

6: kd> dt pdc!\_PDC\_RESILIENCY\_CLIENT fffff802527fe750

   +0x000 Context          : \_PDC\_COMMON\_CONTEXT

   +0x028 ResiliencyType   : 3 ( PdcDamResiliency )

   +0x030 ClientReferences : 0

   +0x038 CurrentState     : 0 ( ResiliencyClientPassive )

   +0x03c NextState        : 1 ( ResiliencyClientActive )

   +0x040 OneTimeTransaction : 0 ''

   +0x044 CurrentTransactionId : 0x654b

   +0x030 AnyNetworks      : \_LIST\_ENTRY [ 0x00000000`00000000 - 0x00000001`00000000 ]

   +0x048 PoResiliency     : 0 ( PoInvalidResiliency )

   +0x04c ClientId         : 4

6: kd> !irql

Debugger saved IRQL for processor 0x6 -- 0 (LOW\_LEVEL)

6: kd> !verifier

Verify Flags Level 0x00000000

  STANDARD FLAGS:

    [ ] (0x00000000) Automatic Checks

    [ ] (0x00000001) Special pool

    [ ] (0x00000002) Force IRQL checking

    [ ] (0x00000008) Pool tracking

    [ ] (0x00000010) I/O verification

    [ ] (0x00000020) Deadlock detection

    [ ] (0x00000080) DMA checking

    [ ] (0x00000100) Security checks

    [ ] (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

    [X] Indicates flag is enabled

Summary of All Verifier Statistics

  RaiseIrqls           0x0

  AcquireSpinLocks     0x0

  Synch Executions     0x0

  Trims                0x0

  Pool Allocations Attempted             0x0

  Pool Allocations Succeeded             0x0

  Pool Allocations Succeeded SpecialPool 0x0

  Pool Allocations With NO TAG           0x0

  Pool Allocations Failed                0x0

  Current paged pool allocations         0x0 for 00000000 bytes

  Peak paged pool allocations            0x0 for 00000000 bytes

  Current nonpaged pool allocations      0x0 for 00000000 bytes

  Peak nonpaged pool allocations         0x0 for 00000000 bytes

6: kd> !sysinfo machineid

Machine ID Information [From Smbios 3.3, DMIVersion 0, Size=4254]

BiosMajorRelease = 15

BiosMinorRelease = 3

FirmwareMajorRelease = 61

FirmwareMinorRelease = 48

BiosVendor = Insyde

BiosVersion = F.03

BiosReleaseDate = 11/17/2021

SystemManufacturer = HP

SystemProductName = HP ENVY x360 Convertible 15m-es1xxx

SystemFamily = 103C\_5335M8 HP Envy

SystemVersion = Type1ProductConfigId

SystemSKU = 4N743UA#ABA

BaseBoardManufacturer = HP

BaseBoardProduct = 8982

BaseBoardVersion = 61.48

kd> dt pdc!\_PDC\_RESILIENCY\_CLIENT

   +0x000 Context          : \_PDC\_COMMON\_CONTEXT

   +0x028 ResiliencyType   : PDC\_RESILIENCY\_TYPE

   +0x030 ClientReferences : Uint8B

   +0x038 CurrentState     : PDC\_CLIENT\_STATE

   +0x03c NextState        : PDC\_CLIENT\_STATE

   +0x040 OneTimeTransaction : UChar

   +0x044 CurrentTransactionId : Uint4B

   +0x030 AnyNetworks      : \_LIST\_ENTRY

   +0x048 PoResiliency     : \_POWER\_RESILIENCY

   +0x04c ClientId         : Uint4B

6: kd> dt pdc!\_PDC\_14F\_TRIAGE

   +0x000 ClientProcess    : Ptr64 \_EPROCESS

   +0x008 CallbackThread   : Ptr64 \_ETHREAD

<https://hsdes.intel.com/appstore/article/#/22018569432>

[MTL-P] [PST] netadaptercx.sys Break in POWER\_DOWN\_netadaptercx!NxTranslationApp::StopDatapath:

NetAdapterCx Is blocking D3 (for S4) IRP processing waiting for the data path to stop and Rx Queue is waiting for its rings to be empty  but there are no pending OIDs or NLBs for the miniport.

Is miniport expected to do something or this is NetAdapterCx Issue?

**5: 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: ffffae0f8fe450a0, Physical Device Object of the stack**

**Arg3: fffff98b2e0cf768, nt!TRIAGE\_9F\_POWER on Win7 and higher, otherwise the Functional Device Object of the stack**

**Arg4: ffffae0fab28c5e0, The blocked IRP**

**5: kd> !irp ffffae0fab28c5e0**

**Irp is active with 8 stacks 7 is current (= 0xffffae0fab28c860)**

**No Mdl: No System Buffer: Thread 00000000:  Irp stack trace.**

**cmd  flg cl Device   File     Completion-Context**

**…**

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

**0 e1 ffffae0fab56aa60 00000000 fffff8007c9bf170-ffffae0fab69b798 Success Error Cancel pending**

**\Driver\e1dnexpress nt!PopRequestCompletion**

**Args: 00015500 00000001 00000004 00000003**

**[N/A(0), N/A(0)]**

**0  0 00000000 00000000 00000000-ffffae0fab69b798**

**Args: 00000000 00000000 00000000 00000000**

**5: kd> !devstack ffffae0fab56aa60**

**!DevObj           !DrvObj            !DevExt           ObjectName**

**> ffffae0fab56aa60  \Driver\e1dnexpressffffae0faaf25310**

**ffffae0f8bf0cdf0  \Driver\ACPI       ffffae0f8bf1a010**

**ffffae0f8fe450a0  \Driver\pci        ffffae0f8fe451f0  NTPNP\_PCI0031**

**!DevNode ffffae0f8ffd38a0 :**

**DeviceInst is "PCI\VEN\_8086&DEV\_550A&SUBSYS\_00008086&REV\_10\3&11583659&0&FE"**

**ServiceName is "e1dnexpress"**

**5: kd> !poaction**

**PopAction: fffff8007d4288a0**

**State..........: 3 - Set System State**

**Updates........: 0**

**Action.........: Sleep**

**Lightest State.: Hibernate**

**Flags..........: 80000004 OverrideApps|Critical**

**Irp minor......: SetPower**

**System State...: Hibernate**

**Hiber Context..: ffffae0f8bf9e620**

**Allocated power irps (PopIrpList - fffff8007d429110)**

**IRP: ffffae0fab9ef920 (wait-wake/S4), PDO: ffffae0fabb842c0**

**IRP: ffffae0fb182a010 (wait-wake/S4), PDO: ffffae0fabb84c40**

**IRP: ffffae0fad86c3f0 (set/S4), PDO: ffffae0f8fe450a0, CURRENT: ffffae0fab56aa60, NOTIFY: ffffae0f8ffd3940**

**IRP: ffffae0fab28c5e0 (set/D3,), PDO: ffffae0f8fe450a0, CURRENT: ffffae0fab56aa60**

**IRP: ffffae0fb3f25010 (wait-wake/S4), PDO: ffffae0f8fe450a0**

**IRP: ffffae0fb11d47d0 (wait-wake/S4), PDO: ffffae0f8fd07e10**

**IRP: ffffae0fa970d010 (wait-wake/S4), PDO: ffffae0fabb86300**

**IRP: ffffae0fb577e280 (wait-wake/S4), PDO: ffffae0f8fe6f360**

**IRP: ffffae0fb1dc3280 (wait-wake/S4), PDO: ffffae0f8fe6d360**

**Irp worker threads (PopIrpThreadList - fffff8007d425cc0)**

**THREAD: ffffae0f8bf23080 (static), IRP: ffffae0fab28c5e0, DEVICE: ffffae0fab56aa60**

**…**

**5: kd> !thread 0xffffae0f8bf23080**

**THREAD ffffae0f8bf23080  Cid 0004.0010  Teb: 0000000000000000 Win32Thread: 0000000000000000 WAIT: (Executive) KernelMode Non-Alertable**

**ffffae0faae18ed8  NotificationEvent**

**Not impersonating**

**DeviceMap                 ffffe78a80233b50**

**Owning Process            ffffae0f8beb0040       Image:         System**

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

**Wait Start TickCount      289935         Ticks: 19199 (0:00:04:59.984)**

**Context Switch Count      4312           IdealProcessor: 0**

**UserTime                  00:00:00.000**

**KernelTime                00:00:01.281**

**Win32 Start Address nt!PopIrpWorker (0xfffff8007c9ee1a0)**

**Stack Init fffff98b2e017bb0 Current fffff98b2e016c20**

**Base fffff98b2e018000 Limit fffff98b2e011000 Call 0000000000000000**

**Priority 13 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5**

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

**fffff98b`2e016c60 fffff800`7c8557e5     : 00000000`0000001b 00000000`00000000 00000000`00000000 00000000`00000000 : nt!KiSwapContext+0x76**

**fffff98b`2e016da0 fffff800`7c857317     : ffffae0f`8bf23080 ffff9781`ec198180 fffff98b`2e016fd0 ffffae0f`ab5391c0 : nt!KiSwapThread+0x1075**

**fffff98b`2e016ec0 fffff800`7c857f37     : 00000000`00000000 ffffae0f`00000000 00000000`00000000 00000000`00000000 : nt!KiCommitThreadWait+0x147**

**fffff98b`2e016f60 fffff800`99b3f908     : ffffae0f`aae18ed8 00000000`00000000 00000000`00000000 00000000`00000000 : nt!KeWaitForSingleObject+0x667**

**(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : netadaptercx!KWaitEventBase<wistd::integral\_constant<enum \_EVENT\_TYPE,0> >::Wait+0x28 (Inline Function @ fffff800`99b3f908)**

**(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : netadaptercx!QueueControl::StopQueues+0x35 (Inline Function @ fffff800`99b3f908)**

**fffff98b`2e017040 fffff800`99b15a49     : 00000000`00000000 ffffae0f`ab284030 00000000`00000002 00000000`00000002 : netadaptercx!NxTranslationApp::StopDatapath+0x10c**

**fffff98b`2e017090 fffff800`99af82ee     : 00000000`00700198 00000000`0000000e 00000000`00000001 00000000`00000002 : netadaptercx!NetClientAdapterStopDatapath+0x9**

**fffff98b`2e0170c0 fffff800`99af8209     : ffffae0f`aaf26050 00000000`00000000 00000000`00000000 00000000`00000000 : netadaptercx!NxAdapter::DatapathStop+0x46**

**fffff98b`2e0170f0 fffff800`99b12a39     : 00000000`0000000d 00000000`00000000 00000000`00000000 fffff800`99b12fae : netadaptercx!NxAdapterStateMachine<NxAdapter>::EntryFuncs::DatapathRestartStoppingEntry+0x9**

**(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : netadaptercx!SmFx::StateMachineEngine::StateMachineEngineImpl::InvokeStateEntryFunction+0x2c (Inline Function @ fffff800`99b12a39)**

**fffff98b`2e017120 fffff800`99b13842     : ffffae0f`aaf26050 00000000`00000000 00000000`00000004 00000000`00000003 : netadaptercx!SmFx::StateMachineEngine::StateMachineEngineImpl::ExecuteCurrentState+0x81**

**fffff98b`2e0171a0 fffff800`99b1256b     : ffffae0f`aaf26050 00000000`00000001 00000000`00000002 00000000`00000000 : netadaptercx!SmFx::StateMachineEngine::StateMachineEngineImpl::ProcessEventQueue+0x13a**

**(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : netadaptercx!SmFx::StateMachineEngine::StateMachineEngineImpl::EnqueueEvent+0xdd (Inline Function @ fffff800`99b1256b)**

**fffff98b`2e0171f0 fffff800`99af4dbc     : ffffae0f`aaf32aa0 00000000`00000001 00000000`00000000 fffff800`99b13610 : netadaptercx!SmFx::StateMachineEngine::EnqueueEvent+0xfb**

**(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : netadaptercx!NxAdapterStateMachine<NxAdapter>::EnqueueEvent+0xa (Inline Function @ fffff800`99af4dbc)**

**(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : netadaptercx!AdapterPnpPower::StopIoD3+0x26 (Inline Function @ fffff800`99af4dbc)**

**fffff98b`2e017230 fffff800`99b12a39     : 00000000`00000014 00000000`00000000 00000000`00000000 fffff800`99b12fae : netadaptercx!AdapterPnpPowerStateMachine<AdapterPnpPower>::EntryFuncs::InterfaceStartedGoingToIoStoppedD3Entry+0x2c**

**(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : netadaptercx!SmFx::StateMachineEngine::StateMachineEngineImpl::InvokeStateEntryFunction+0x2c (Inline Function @ fffff800`99b12a39)**

**fffff98b`2e017270 fffff800`99b13842     : ffffae0f`ab294b70 ffffae0f`aafc9a00 00000000`00000003 00000000`00000002 : netadaptercx!SmFx::StateMachineEngine::StateMachineEngineImpl::ExecuteCurrentState+0x81**

**fffff98b`2e0172f0 fffff800`99b1256b     : ffffae0f`ab294b70 ffffae0f`aafc9a01 00000000`0000000a 00000000`00000000 : netadaptercx!SmFx::StateMachineEngine::StateMachineEngineImpl::ProcessEventQueue+0x13a**

**(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : netadaptercx!SmFx::StateMachineEngine::StateMachineEngineImpl::EnqueueEvent+0xdd (Inline Function @ fffff800`99b1256b)**

**fffff98b`2e017340 fffff800`99af60bf     : ffffae0f`aaf32aa0 ffffae0f`aafc9ab0 ffffae0f`aaf328c0 00000000`00000000 : netadaptercx!SmFx::StateMachineEngine::EnqueueEvent+0xfb**

**(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : netadaptercx!AdapterPnpPowerStateMachine<AdapterPnpPower>::EnqueueEvent+0xd (Inline Function @ fffff800`99af60bf)**

**(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : netadaptercx!AdapterPnpPower::IoStop+0x1e (Inline Function @ fffff800`99af60bf)**

**(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : netadaptercx!DevicePnpPower::PoweringDownD3::\_\_l2::<lambda\_8290f65210c314f913c9802f5c9fe611>::operator()+0x1e (Inline Function @ fffff800`99af60bf)**

**(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : netadaptercx!NxCollection<NxAdapter>::ForEach+0x4f (Inline Function @ fffff800`99af60bf)**

**(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : netadaptercx!DevicePnpPower::PoweringDownD3+0x56 (Inline Function @ fffff800`99af60bf)**

**fffff98b`2e017380 fffff800`99b12a39     : ffffae0f`aaf264a0 00000000`00000001 00000000`00000000 fffff800`99b2fea0 : netadaptercx!DevicePnpPowerStateMachine<DevicePnpPower>::EntryFuncs::PoweringDownD3Entry+0x6f**

**(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : netadaptercx!SmFx::StateMachineEngine::StateMachineEngineImpl::InvokeStateEntryFunction+0x2c (Inline Function @ fffff800`99b12a39)**

**fffff98b`2e0173e0 fffff800`99b13842     : ffffae0f`aaf264a0 fffff98b`2e017700 00000000`0000000a 00000000`00000009 : netadaptercx!SmFx::StateMachineEngine::StateMachineEngineImpl::ExecuteCurrentState+0x81**

**fffff98b`2e017460 fffff800`99b1256b     : ffffae0f`aaf264a0 fffff98b`2e017701 00000000`00000007 00000000`00000000 : netadaptercx!SmFx::StateMachineEngine::StateMachineEngineImpl::ProcessEventQueue+0x13a**

**(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : netadaptercx!SmFx::StateMachineEngine::StateMachineEngineImpl::EnqueueEvent+0xdd (Inline Function @ fffff800`99b1256b)**

**fffff98b`2e0174b0 fffff800`99af5d3c     : ffffae0f`aafc9ab0 fffff98b`2e017700 00000000`00000000 00000000`00000000 : netadaptercx!SmFx::StateMachineEngine::EnqueueEvent+0xfb**

**(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : netadaptercx!KWaitEventBase<wistd::integral\_constant<enum \_EVENT\_TYPE,1> >::Wait+0x5 (Inline Function @ fffff800`99af5d3c)**

**fffff98b`2e0174f0 fffff800`99b03713     : 00000000`00000000 ffffae0f`aaf25350 00000000`00000000 00000000`00000000 : netadaptercx!DevicePnpPower::ChangePowerState+0x48**

**fffff98b`2e017530 fffff800`7fd8e031     : ffffae0f`aaf25928 fffff98b`2e017700 00000000`00000000 ffffae0f`aaf25628 : netadaptercx!EvtCxDevicePreD0ExitPreHardwareDisabled+0x53**

**fffff98b`2e017560 fffff800`7fd3a52e     : ffffae0f`ab5d5d70 00000000`00000000 fffff98b`00000001 fffff800`7fd3ac04 : Wdf01000!FxPnpDeviceD0ExitPreHwDisabled::InvokeCxCallback+0x31**

**fffff98b`2e0175c0 fffff800`7fd3a46f     : ffffae0f`aaf25928 ffffae0f`aaf25020 ffffae0f`aaf25350 00000000`0000000e : Wdf01000!FxPrePostCallback::IssuePreCxCallbacksStateless+0x7a**

**fffff98b`2e0175f0 fffff800`7fd3a10c     : 00000000`00000000 00000000`00000004 00000000`00000015 fffff800`7fd17ebf : Wdf01000!FxPrePostCallback::InvokeStateless+0x5f**

**5: kd> !thread ffffae0fab539080**

**THREAD ffffae0fab539080  Cid 0004.03b8  Teb: 0000000000000000 Win32Thread: 0000000000000000 WAIT: (Executive) KernelMode Non-Alertable**

**ffffae0fb1f7ca70  NotificationEvent**

**Not impersonating**

**DeviceMap                 ffffe78a80233b50**

**Owning Process            ffffae0f8beb0040       Image:         System**

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

**Wait Start TickCount      289935         Ticks: 19199 (0:00:04:59.984)**

**Context Switch Count      5851           IdealProcessor: 11  NoStackSwap**

**UserTime                  00:00:00.000**

**KernelTime                00:00:00.390**

**Win32 Start Address nt!ExpWorkerThread (0xfffff8007c98ce90)**

**Stack Init fffff98b2f158bb0 Current fffff98b2f1583a0**

**Base fffff98b2f159000 Limit fffff98b2f152000 Call 0000000000000000**

**Priority 13 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5**

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

**fffff98b`2f1583e0 fffff800`7c8557e5     : 00000000`0000001b 00000000`00000000 00000000`00000000 00000000`00000000 : nt!KiSwapContext+0x76**

**fffff98b`2f158520 fffff800`7c857317     : ffffae0f`ab539080 ffff9781`ec3c6180 fffff98b`2f158750 ffffae0f`00070000 : nt!KiSwapThread+0x1075**

**fffff98b`2f158640 fffff800`7c857f37     : fffff98b`00000000 fffff800`00000000 00000000`00000000 00000000`00000000 : nt!KiCommitThreadWait+0x147**

**fffff98b`2f1586e0 fffff800`99b1e849     : ffffae0f`b1f7ca70 ffffae0f`00000000 fffff800`99b37600 00000000`00000000 : nt!KeWaitForSingleObject+0x667**

**(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : netadaptercx!KWaitEventBase<wistd::integral\_constant<enum \_EVENT\_TYPE,0> >::Wait+0x2e (Inline Function @ fffff800`99b1e849)**

**fffff98b`2f1587c0 fffff800`99b40a9c     : 00000000`00000000 00000000`00000000 00000000`00000002 fffff800`7c83e1f7 : netadaptercx!Queue::Stop+0x51**

**fffff98b`2f158800 fffff800`99b40c57     : ffffae0f`aae02c00 fffff800`99b37670 ffffae0f`aae18e80 00000000`00000000 : netadaptercx!QueueControl::SynchronizeDatapathState+0xf4**

**fffff98b`2f158850 fffff800`99b18142     : ffffae0f`aae02c00 00000000`00000000 ffffae0f`aa993570 ffffae0f`8bf23080 : netadaptercx!QueueControl::SynchronizeDatapathWork+0x63**

**(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : netadaptercx!IoWorkItem<QueueControl,{QueueControl::SynchronizeDatapathWork,0},\_DRIVER\_OBJECT>::Invoke+0xe (Inline Function @ fffff800`99b18142)**

**fffff98b`2f1588a0 fffff800`7c8d3f71     : ffffae0f`a9c3e4f0 00000000`00000000 ffffae0f`aa993570 fffff800`7d575b40 : netadaptercx!IoWorkItem<QueueControl,{QueueControl::SynchronizeDatapathWork,0},\_DRIVER\_OBJECT>::CallbackThunk+0x12**

**fffff98b`2f1588d0 fffff800`7c98cfe5     : ffffae0f`8bfb4c80 ffffae0f`ab539080 fffff98b`2f158a40 00004c4c`00000000 : nt!IopProcessWorkItem+0x141**

**fffff98b`2f158940 fffff800`7c8dcf77     : ffffae0f`ab539080 00000000`00000001 ffffae0f`ab539080 fffff800`7c98ce90 : nt!ExpWorkerThread+0x155**

**fffff98b`2f158b30 fffff800`7ca86d14     : ffff9781`ec324180 ffffae0f`ab539080 fffff800`7c8dcf20 00000000`0000514d : nt!PspSystemThreadStartup+0x57**

**fffff98b`2f158b80 00000000`00000000     : fffff98b`2f159000 fffff98b`2f152000 00000000`00000000 00000000`00000000 : nt!KiStartSystemThread+0x34**

**5: kd> !ndiskd.miniports**

**Driver             NetAdapter          Name**

**…**

**ffffae0fa9b28020   ffffae0fab284030    Intel(R) Ethernet Connection (18) I219-LM**

**5: kd> !ndiskd.oid -miniport ffffae0fab284030**

**ALL PENDING OIDs**

**[Showing all OIDs on the stack for miniport ffffae0fab284030]**

**No pending or queued OIDs were found.**

**5: kd> !ndiskd.pendingnbls ffffae0fab284030**

**PHASE 1/3: Found 56 NBL pool(s).**

**PHASE 2/3: Found 527 freed NBL(s).**

**Pending Nbl        Currently held by**

**PHASE 3/3: Found 0 pending NBL(s) of 18955 total NBL(s).**

**Search complete.**

I see it's marked as "Ignored", seems like driver marked it as ignored, but didn't transfer ownership to the OS by moving the indices, so queues don't stop waiting for this to happen.

<https://hsdes.intel.com/appstore/article/#/14019831212>

[MTL-P 682][C0][DPMO][S0ix] BSOD BAD\_POOL\_CALLER (c2) - Module name: USB4DeviceRouter during S0ix cycling:

Usb4DeviceRouter!Usb4Drd::Router::CompleteGrandmasterTimeRequest does not check if m\_TimePostingRequests list is empty and attempts to delete list head resulting in Bugcheck BAD\_POOL\_CALLER (c2) – see attached memory dump:

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

**BAD\_POOL\_CALLER (c2)**

**The current thread is making a bad pool request.  Typically this is at a bad IRQL level or double freeing the same allocation, etc.**

**Arguments:**

**Arg1: 0000000000000099, Attempt to free pool with invalid address  (or corruption in pool header)**

**Arg2: ffff838763b9f228, Address being freed**

**Arg3: 0000000000000000, 0**

**Arg4: 0000000000000000, 0**

Callstack indicates that Usb4DeviceRouter!Usb4Drd::Router::CompleteGrandmasterTimeRequest attempts to pop a node from the m\_TimePostingRequests list:

**0: kd> k**

**# Child-SP          RetAddr               Call Site**

**00 fffff800`4c4ffb08 fffff800`47cae03e     nt!KeBugCheckEx**

**01 fffff800`4c4ffb10 fffff800`5102cfea     nt!ExFreePoolWithTag+0x7de**

**02 (Inline Function) --------`--------     Usb4DeviceRouter!operator delete+0x23**

**03 (Inline Function) --------`--------     Usb4DeviceRouter!operator delete+0x23**

**04 (Inline Function) --------`--------     Usb4DeviceRouter!utl::allocator<utl::\_DlistNode<WDFREQUEST\_\_ \*> >::deallocate+0x23**

**05 (Inline Function) --------`--------     Usb4DeviceRouter!utl::allocator\_traits<utl::allocator<utl::\_DlistNode<WDFREQUEST\_\_ \*> > >::deallocate+0x23**

**06 (Inline Function) --------`--------     Usb4DeviceRouter!utl::\_ContainerBase<WDFREQUEST\_\_ \*,utl::allocator<WDFREQUEST\_\_ \*> >::\_DeleteNode+0x23**

**07 (Inline Function) --------`--------     Usb4DeviceRouter!utl::list<WDFREQUEST\_\_ \*,utl::allocator<WDFREQUEST\_\_ \*> >::erase+0x23**

**08 (Inline Function) --------`--------     Usb4DeviceRouter!utl::list<WDFREQUEST\_\_ \*,utl::allocator<WDFREQUEST\_\_ \*> >::pop\_front+0x23**

**09 fffff800`4c4ffba0 fffff800`510356db     Usb4DeviceRouter!Usb4Drd::Router::CompleteGrandmasterTimeRequest+0x46**

**0a (Inline Function) --------`--------     Usb4DeviceRouter!Usb4Drd::Router::CompleteGrandmasterTimeRequestSucceeded+0x7**

**0b fffff800`4c4ffbe0 fffff800`51040028     Usb4DeviceRouter!Usb4Drd::RouterStateMachine<Usb4Drd::Router>::EntryFuncs::CompletingGrandMasterTimeRequestEntry+0xb**

**0c (Inline Function) --------`--------     Usb4DeviceRouter!SmFx::StateMachineEngine::StateMachineEngineImpl::InvokeStateEntryFunction+0x2c**

**0d fffff800`4c4ffc10 fffff800`5104085c     Usb4DeviceRouter!SmFx::StateMachineEngine::StateMachineEngineImpl::ExecuteCurrentState+0x84**

**0e fffff800`4c4ffc90 fffff800`5103f9e3     Usb4DeviceRouter!SmFx::StateMachineEngine::StateMachineEngineImpl::ProcessEventQueue+0x138**

**0f (Inline Function) --------`--------     Usb4DeviceRouter!SmFx::StateMachineEngine::StateMachineEngineImpl::EnqueueEvent+0xdd**

**10 fffff800`4c4ffce0 fffff800`51027afe     Usb4DeviceRouter!SmFx::StateMachineEngine::EnqueueEvent+0xfb**

**11 (Inline Function) --------`--------     Usb4DeviceRouter!Usb4Drd::RouterStateMachine<Usb4Drd::Router>::EnqueueEvent+0xb**

**12 fffff800`4c4ffd20 fffff800`50fdac12     Usb4DeviceRouter!Usb4Drd::Router::EvtConfigSpaceAccessComplete+0xde**

**13 fffff800`4c4ffd90 fffff800`4c6c6e26     Usb4DeviceRouter!Usb4Drd::HostRouterInterface::EvtReadWriteRequestCompletion+0x5f2**

**14 fffff800`4c4ffed0 fffff800`4c6c6b5a     Wdf01000!FxRequestBase::CompleteSubmitted+0xba**

**15 (Inline Function) --------`--------     Wdf01000!FxIoTarget::CompleteRequest+0x8**

**16 fffff800`4c4fff10 fffff800`4c6c7285     Wdf01000!FxIoTarget::RequestCompletionRoutine+0xba**

**17 fffff800`4c4fff70 fffff800`4755a8f6     Wdf01000!FxIoTarget::\_RequestCompletionRoutine+0x35**

**18 fffff800`4c4fffa0 fffff800`474993c4     nt!IopUnloadSafeCompletion+0x56**

**19 fffff800`4c4fffd0 fffff800`47499277     nt!IopfCompleteRequest+0x134**

**1a fffff800`4c5000b0 fffff800`4c6c3cc6     nt!IofCompleteRequest+0x17**

**1b (Inline Function) --------`--------     Wdf01000!FxIrp::CompleteRequest+0x13**

**1c fffff800`4c5000e0 fffff800`4c6c3a51     Wdf01000!FxRequest::CompleteInternal+0x246**

**1d (Inline Function) --------`--------     Wdf01000!FxRequest::Complete+0x31**

**1e (Inline Function) --------`--------     Wdf01000!FxRequest::CompleteWithInformation+0x3c**

**1f fffff800`4c500170 fffff800`76d184c9     Wdf01000!imp\_WdfRequestCompleteWithInformation+0xa1**

**20 (Inline Function) --------`--------     Usb4HostRouter!WdfRequestCompleteWithInformation+0x27**

**21 fffff800`4c5001d0 fffff800`76d13f03     Usb4HostRouter!Usb4Hrd::IoctlConfigSpaceAccessReadRequest::Complete+0x329**

**22 (Inline Function) --------`--------     Usb4HostRouter!Usb4Hrd::ConfigSpaceAccessor::CompleteRequests+0x2f**

**23 fffff800`4c5002e0 fffff800`4c6e3afc     Usb4HostRouter!Usb4Hrd::ConfigSpaceAccessor::RequestCompletionDpcCallback+0x63**

**24 fffff800`4c500320 fffff800`4c6e3b1c     Wdf01000!FxDpc::DpcHandler+0xc0**

**25 fffff800`4c500360 fffff800`474a7a4c     Wdf01000!FxDpc::FxDpcThunk+0xc**

**26 fffff800`4c500390 fffff800`474a6a3a     nt!KiExecuteAllDpcs+0x42c**

**27 fffff800`4c5008d0 fffff800`4763107e     nt!KiRetireDpcList+0x1ba**

**28 fffff800`4c500b80 00000000`00000000     nt!KiIdleLoop+0x9e**

From the calling frame, we can determine the address passed to nt!ExFreePoolWithTag to cross-reference with Bugcheck parameter:

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

**02 (Inline Function) --------`--------     Usb4DeviceRouter!operator delete+0x23**

**rax=ffff800000000000 rbx=ffff838763b9f220 rcx=00000000000000c2**

**rdx=0000000000000099 rsi=0000000000000000 rdi=0000000000000000**

**rip=fffff8005102cfea rsp=fffff8004c4ffba0 rbp=fffff8004c4ffe00**

**r8=ffff838763b9f228  r9=0000000000000000 r10=fffff80047cad860**

**r11=fffff8004c4ffb98 r12=00000000000000fe r13=0000000000000000**

**r14=ffff8387653a5848 r15=0000000000000002**

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

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

**Usb4DeviceRouter!operator delete+0x23 [inlined in Usb4DeviceRouter!Usb4Drd::Router::CompleteGrandmasterTimeRequest+0x46]:**

**fffff800`5102cfea 48ff4b18        dec     qword ptr [rbx+18h] ds:002b:ffff8387`63b9f238=0000000000000000**

**0: kd> ub**

**Usb4DeviceRouter!operator delete [inlined in Usb4DeviceRouter!Usb4Drd::Router::CompleteGrandmasterTimeRequest+0x23]:**

**fffff800`5102cfc7 ba55344452      mov     edx,52443455h**

**fffff800`5102cfcc 4c8b4108        mov     r8,qword ptr [rcx+8]**

**fffff800`5102cfd0 488b01          mov     rax,qword ptr [rcx]**

**fffff800`5102cfd3 488b7110        mov     rsi,qword ptr [rcx+10h]**

**fffff800`5102cfd7 498900          mov     qword ptr [r8],rax**

**fffff800`5102cfda 4c894008        mov     qword ptr [rax+8],r8**

**fffff800`5102cfde 4c8b159bc10300  mov     r10,qword ptr [Usb4DeviceRouter!\_imp\_ExFreePoolWithTag (fffff800`51069180)]**

**fffff800`5102cfe5 e87608c8f6      call    nt!ExFreePoolWithTag (fffff800`47cad860)**

**0: kd> ub fffff800`5102cfc7**

**Usb4DeviceRouter!Usb4Drd::Router::CompleteGrandmasterTimeRequest+0x7:**

**fffff800`5102cfab 48897020        mov     qword ptr [rax+20h],rsi**

**fffff800`5102cfaf 57              push    rdi**

**fffff800`5102cfb0 4883ec30        sub     rsp,30h**

**fffff800`5102cfb4 4883600800      and     qword ptr [rax+8],0**

**fffff800`5102cfb9 488bd9          mov     rbx,rcx**

**fffff800`5102cfbc 488b4908        mov     rcx,qword ptr [rcx+8]**

**fffff800`5102cfc0 8bfa            mov     edi,edx**

**fffff800`5102cfc2 4883601800      and     qword ptr [rax+18h],0**

The address is the “next” pointer from the m\_TimePostingRequests list, but the list is empty:

**0: kd> dq ffff838763b9f220+8 L2**

**ffff8387`63b9f228  ffff8387`63b9f228 ffff8387`63b9f228**

The ffff8387`63b9f228 is part of the larger allocation which starts at ffff838763b9f220:

**0: kd> !pool  ffff8387`63b9f228**

**Pool page ffff838763b9f228 region is Nonpaged pool**

**\*ffff838763b9f210 size:  500 previous size:    0  (Allocated) \*U4DR**

**Owning component : Unknown (update pooltag.txt)**

**ffff838763b9f720 size:  880 previous size:    0  (Allocated)  PciB**

**ffff838763b9ffa0 size:   40 previous size:    0  (Free)       XMB.**

The ffff838763b9f220 is the “this” pointer to Usb4DeviceRouter!Usb4Drd::Router:

**0: kd> .frame /r 9**

**09 fffff800`4c4ffba0 fffff800`510356db     Usb4DeviceRouter!Usb4Drd::Router::CompleteGrandmasterTimeRequest+0x46**

**rax=ffff800000000000 rbx=ffff838763b9f220 rcx=00000000000000c2**

**rdx=0000000000000099 rsi=0000000000000000 rdi=0000000000000000**

**rip=fffff8005102cfea rsp=fffff8004c4ffba0 rbp=fffff8004c4ffe00**

**r8=ffff838763b9f228  r9=0000000000000000 r10=fffff80047cad860**

**r11=fffff8004c4ffb98 r12=00000000000000fe r13=0000000000000000**

**r14=ffff8387653a5848 r15=0000000000000002**

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

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

**Usb4DeviceRouter!Usb4Drd::Router::CompleteGrandmasterTimeRequest+0x46:**

**fffff800`5102cfea 48ff4b18        dec     qword ptr [rbx+18h] ds:002b:ffff8387`63b9f238=0000000000000000**

**0: kd> dv /V**

**@rbx              @rbx                         this = 0xffff8387`63b9f220**

**@edi              @edi               CompleteStatus = 0n0**

**fffff800`4c4ffbe0 @rsp+0x0040                buffer = 0x00000000`00000000**

**fffff800`4c4ffbf0 @rsp+0x0050                length = 0**

**<unavailable>     <unavailable>              status = <value unavailable>**

**@rsi              @rsi                      request = 0x00000000`00000000**

**0: kd> dt this m\_TimePostingRequests**

**Local var @ rbx Type Usb4Drd::Router\***

**+0x008 m\_TimePostingRequests : utl::list<WDFREQUEST\_\_ \*,utl::allocator<WDFREQUEST\_\_ \*> >**

<https://hsdes.intel.com/appstore/article/#/22018534508>

[MTLH][GCS][ADSP] IntcOED/IntcSDW BUS driver fails rollback test due to PAGE\_FAULT:

IntcSdwBus passes NULL to the ObDereferenceObject, this issue should be dispatched to the owners of the IntcSdwBus.sys driver.  
  
**18: kd> !analyze -show**

**PAGE\_FAULT\_IN\_NONPAGED\_AREA (50)**

**Invalid system memory was referenced.  This cannot be protected by try-except.**

**Typically the address is just plain bad or it is pointing at freed memory.**

**Arguments:**

**Arg1: ffffffffffffffd0, memory referenced.**

**Arg2: 0000000000000002, X64: bit 0 set if the fault was due to a not-present PTE.**

**bit 1 is set if the fault was due to a write, clear if a read.**

**bit 3 is set if the processor decided the fault was due to a corrupted PTE.**

**bit 4 is set if the fault was due to attempted execute of a no-execute PTE.**

**- ARM64: bit 1 is set if the fault was due to a write, clear if a read.**

**bit 3 is set if the fault was due to attempted execute of a no-execute PTE.**

**Arg3: fffff8011e12ccc6, If non-zero, the instruction address which referenced the bad memory**

**address.**

**Arg4: 0000000000000002, (reserved)**

**18: kd> k**

**# Child-SP          RetAddr               Call Site**

**00 ffffd588`662d6598 fffff801`1e3c2002     nt!DbgBreakPointWithStatus**

**01 ffffd588`662d65a0 fffff801`1e3c16bc     nt!KiBugCheckDebugBreak+0x12**

**02 ffffd588`662d6600 fffff801`1e223db7     nt!KeBugCheck2+0xc0c**

**03 ffffd588`662d6d80 fffff801`1e3135ad     nt!KeBugCheckEx+0x107**

**04 ffffd588`662d6dc0 fffff801`1e1146ab     nt!MiSystemFault+0x240c8d**

**05 ffffd588`662d6ed0 fffff801`1e27a8ba     nt!MmAccessFault+0x44b**

**06 ffffd588`662d7050 fffff801`1e12ccc6     nt!KiPageFault+0x37a**

**07 (Inline Function) --------`--------     nt!ObpDecrPointerCountRelease+0x7**

**08 (Inline Function) --------`--------     nt!ObfDereferenceObjectWithTag+0x17**

**09 ffffd588`662d71e0 fffff801`3f741462     nt!ObfDereferenceObject+0x26**

**0a ffffd588`662d7220 fffff801`3f72d94a     IntcSdwBus!soundwire::Manager::ReleaseHwCodecPdoList+0x7e**

**0b ffffd588`662d7270 fffff801`3f615d34     IntcSdwBus!soundwire::SdwOedIface\_ReleaseHwCodecPdoList+0x9a**

**0c ffffd588`662d72c0 fffff801`232115ff     IntcOED!COESoundWireVirtualBus::QueryDeviceRelations+0x294**

**0d (Inline Function) --------`--------     Wdf01000!PreprocessIrp+0x35**

**0e (Inline Function) --------`--------     Wdf01000!DispatchWorker+0x17f**

**0f (Inline Function) --------`--------     Wdf01000!FxDevice::Dispatch+0x198**

**10 ffffd588`662d7370 fffff801`1e12a955     Wdf01000!FxDevice::DispatchWithLock+0x1cf**

**11 (Inline Function) --------`--------     nt!IopfCallDriver+0x40**

**12 ffffd588`662d73d0 fffff801`3f4f1dc3     nt!IofCallDriver+0x55**

**13 ffffd588`662d7410 fffff801`3f52e525     portcls!ForwardIrpAsynchronous+0x53**

**14 ffffd588`662d7440 fffff801`3f52eb8b     portcls!DispatchPnp+0x105**

**15 ffffd588`662d74d0 fffff801`3f7822ea     portcls!PcDispatchIrp+0x1fb**

**16 ffffd588`662d7540 fffff801`1e12a955     IntcSDW!IntcAudDispatchPnp+0x28a**

**17 (Inline Function) --------`--------     nt!IopfCallDriver+0x40**

**18 ffffd588`662d7590 fffff801`3c9b13e5     nt!IofCallDriver+0x55**

**19 ffffd588`662d75d0 fffff801`3c9b1103     ksthunk!CKernelFilterDevice::DispatchIrp+0xf5**

**1a ffffd588`662d7630 fffff801`1e12a955     ksthunk!CKernelFilterDevice::DispatchIrpBridge+0x13**

**1b (Inline Function) --------`--------     nt!IopfCallDriver+0x40**

**1c ffffd588`662d7660 fffff801`1e67841c     nt!IofCallDriver+0x55**

**1d ffffd588`662d76a0 fffff801`1e170010     nt!IopSynchronousCall+0xf8**

**1e ffffd588`662d7710 fffff801`1e674885     nt!PnpSendIrp+0x64**

**1f ffffd588`662d7780 fffff801`1e5f6437     nt!PnpQueryDeviceRelations+0x51**

**20 ffffd588`662d7810 fffff801`1e0b717c     nt!PiQueryPowerRelations+0x4f**

**21 ffffd588`662d7870 fffff801`1e183465     nt!PnpDeviceActionWorker+0x65c**

**22 ffffd588`662d7940 fffff801`1e0bce37     nt!ExpWorkerThread+0x155**

**23 ffffd588`662d7b30 fffff801`1e26d044     nt!PspSystemThreadStartup+0x57**

**24 ffffd588`662d7b80 00000000`00000000     nt!KiStartSystemThread+0x34**

**18: kd> .frame /r a**

**0a ffffd588`662d7220 fffff801`3f72d94a     IntcSdwBus!soundwire::Manager::ReleaseHwCodecPdoList+0x7e**

**rax=0000000000000000 rbx=ffffd588662d7300 rcx=0000000000000000**

**rdx=00000000000000cd rsi=ffffd588662d7300 rdi=00000000662d7380**

**rip=fffff8013f741462 rsp=ffffd588662d7220 rbp=ffffe6836c27eaf0**

**r8=0000000000000000  r9=000000000000001c r10=ffffe6836d0f1000**

**r11=00000000000096a8 r12=fffff8013f715db0 r13=ffffe68364c4ba30**

**r14=fffff8013f71b080 r15=fffff8013f71b080**

**iopl=0         nv up ei ng nz na po nc**

**cs=0010  ss=0018  ds=002b  es=002b  fs=0053  gs=002b             efl=00040286**

**IntcSdwBus!soundwire::Manager::ReleaseHwCodecPdoList+0x7e:**

**fffff801`3f741462 488d5b08        lea     rbx,[rbx+8]**

**18: kd> ub**

**IntcSdwBus!soundwire::Manager::ReleaseHwCodecPdoList+0x5f:**

**fffff801`3f741443 746f            je      IntcSdwBus!soundwire::Manager::ReleaseHwCodecPdoList+0xd0 (fffff801`3f7414b4)**

**fffff801`3f741445 488d8d20040000  lea     rcx,[rbp+420h]**

**fffff801`3f74144c ff15762dfdff    call    qword ptr [IntcSdwBus!\_imp\_ExAcquireFastMutex (fffff801`3f7141c8)]**

**fffff801`3f741452 85ff            test    edi,edi**

**fffff801`3f741454 7416            je      IntcSdwBus!soundwire::Manager::ReleaseHwCodecPdoList+0x88 (fffff801`3f74146c)**

**fffff801`3f741456 488bde          mov     rbx,rsi**

**fffff801`3f741459 488b0b          mov     rcx,qword ptr [rbx]**

**fffff801`3f74145c ff15ee2cfdff    call    qword ptr [IntcSdwBus!\_imp\_ObfDereferenceObject (fffff801`3f714150)]**

**18: kd> dq ffffd588662d7300 L1**

**ffffd588`662d7300  00000000`00000000**

<https://hsdes.intel.com/appstore/article/#/14019795554>

[WS 2022] Enabling Bitlocker on boot drive of size 2TB leads to BSOD:

97: kd> !analyze -show

PAGE\_FAULT\_IN\_NONPAGED\_AREA (50)

Invalid system memory was referenced.  This cannot be protected by try-except.

Typically the address is just plain bad or it is pointing at freed memory.

Arguments:

Arg1: ffffb38dd9a65000, memory referenced.

Arg2: 0000000000000002, value 0 = read operation, 1 = write operation.

Arg3: fffff800280f29d3, If non-zero, the instruction address which referenced the bad memory

      address.

Arg4: 0000000000000000, (reserved)

97: kd> !pool ffffb38dd9a65000

Pool page ffffb38dd9a65000 region is Paged pool

ffffb38dd9a65000 is not a valid large pool allocation, checking large session pool...

ffffb38dd9a65000 is not valid pool. Checking for freed (or corrupt) pool

Address ffffb38dd9a65000 could not be read. It may be a freed, invalid or paged out page

97: kd> k

 # Child-SP          RetAddr               Call Site

00 fffff184`749a18d8 fffff800`2360d087     nt!KeBugCheckEx

01 fffff184`749a18e0 fffff800`2373901e     nt!MiSystemFault+0xa77

02 fffff184`749a19e0 fffff800`2382a841     nt!MmAccessFault+0x2ee

03 fffff184`749a1b80 fffff800`280f29d3     nt!KiPageFault+0x341

04 fffff184`749a1d10 fffff800`28130f83     fvevol!FveWorksetCommit+0x4f

05 fffff184`749a1d40 fffff800`2816d964     fvevol!FveSynchronizeDatasetUpdate+0x2b7

06 fffff184`749a1e10 fffff800`2817903f     fvevol!IoctlFveSetDataset+0x2c0

07 fffff184`749a2150 fffff800`28108e30     fvevol!IoctlFveWorker+0x40f

08 fffff184`749a21f0 fffff800`2376375b     fvevol!FveWorkerAutoWorker+0xa0

09 fffff184`749a2230 fffff800`23719111     nt!IopProcessWorkItem+0xfb

0a fffff184`749a22a0 fffff800`236c8785     nt!ExpWorkerThread+0x161

0b fffff184`749a24b0 fffff800`2381ed48     nt!PspSystemThreadStartup+0x55

0c fffff184`749a2500 00000000`00000000     nt!KiStartSystemThread+0x28

97: kd> .frame /r 4

04 fffff184`749a1d10 fffff800`28130f83     fvevol!FveWorksetCommit+0x4f

rax=0000000000000000 rbx=0000000000000000 rcx=0000000000070000

rdx=ffffe675a5301fc0 rsi=ffffb38dd9a55040 rdi=ffffb38dd9a65000

rip=fffff800280f29d3 rsp=fffff184749a1d10 rbp=ffff9a037ed57000

 r8=0000000000000006  r9=0000000000000000 r10=ffff9a037ed5921e

r11=ffffb38dd9a571f6 r12=ffff9a037bf39850 r13=ffffb38dd9a55000

r14=ffff9a037bf38b50 r15=ffff9a037bf37450

iopl=0         nv up ei pl zr na po nc

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

fvevol!FveWorksetCommit+0x4f:

fffff800`280f29d3 f3aa            rep stos byte ptr [rdi]

97: kd> !pool 0xffffb38d`d9a55040

Pool page ffffb38dd9a55040 region is Paged pool

\*ffffb38dd9a55000 : large page allocation, tag is FVE0, size is 0x10000 bytes

Pooltag FVE0 : General allocations, Binary : fvevol.sys

The changes in fvevol!ActionFveInit implemented in the latest Windows vNext build which fix this issue need to be backported to WS 2022.

<https://hsdes.intel.com/appstore/article/#/18031202832>

[RPL-U-Refresh][HLK][GC][Audio][BT-LE]: Observing Bugcheck-7E (System-Thread-Exception-Not-Handled) pointing to IntcBtLE when running "System-PNP (disable and enable) with IO Before and After (Reliability)" HLK-test:

Acx01000.sys appears to be leaking WDFIOTARGET objects – see attached memory dump:

This is a debug breakpoint:

**0: 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: ffffffff80000003, The exception code that was not handled**

**Arg2: fffff80208e47240, The address that the exception occurred at**

**Arg3: ffff9900395ef128, Exception Record Address**

**Arg4: ffff9900395ee940, Context Record Address**

**0: kd> u fffff80208e47240 L1**

**nt!DbgBreakPoint:**

**fffff802`08e47240 cc              int     3**

As IntcBtLE.sys is unloading, Wdf01000!FxPoolDump has detected a memory leak and triggered debug breakpoint:

**0: kd> k**

**# Child-SP          RetAddr               Call Site**

**00 ffff9900`395ee0b8 fffff802`08e5c984     nt!KeBugCheckEx**

**01 ffff9900`395ee0c0 fffff802`08dfe711     nt!PspSystemThreadStartup$filt$0+0x44**

**02 ffff9900`395ee100 fffff802`08e484ef     nt!\_C\_specific\_handler+0xa1**

**03 ffff9900`395ee170 fffff802`08c5b0d3     nt!RtlpExecuteHandlerForException+0xf**

**04 ffff9900`395ee1a0 fffff802`08d24efe     nt!RtlDispatchException+0x2f3**

**05 ffff9900`395ee910 fffff802`08e529fc     nt!KiDispatchException+0x1ae**

**06 ffff9900`395eeff0 fffff802`08e4b1f9     nt!KiExceptionDispatch+0x13c**

**07 ffff9900`395ef1d0 fffff802`08e47241     nt!KiBreakpointTrap+0x339**

**08 ffff9900`395ef368 fffff802`0a1d83f3     nt!DbgBreakPoint+0x1**

**09 (Inline Function) --------`--------     Wdf01000!Mx::MxDbgBreakPoint+0x7**

**0a ffff9900`395ef370 fffff802`0a205f03     Wdf01000!FxVerifierDbgBreakPoint+0x4b**

**0b ffff9900`395ef3b0 fffff802`0a204393     Wdf01000!FxPoolDump+0x17b**

**0c (Inline Function) --------`--------     Wdf01000!FxPoolDestroy+0x42**

**0d (Inline Function) --------`--------     Wdf01000!FxPoolPackageDestroy+0x46**

**0e ffff9900`395ef450 fffff802`0a200cb7     Wdf01000!FxDestroy+0xc3**

**0f ffff9900`395ef490 fffff806`d89d20f2     Wdf01000!FxDriver::Unload+0xe7**

**10 ffff9900`395ef4e0 fffff802`09226d5c     IntcBtLE+0x20f2**

**11 ffff9900`395ef510 fffff802`091f256a     nt!IopUnloadDriver+0x224**

**12 ffff9900`395ef640 fffff802`08db61f1     nt!PnpUnloadAttachedDriver+0xa6**

**13 ffff9900`395ef690 fffff802`0923935a     nt!PnpRemoveLockedDeviceNode+0x249**

**14 ffff9900`395ef6f0 fffff802`09239027     nt!PnpDeleteLockedDeviceNode+0x4e**

**15 ffff9900`395ef730 fffff802`0923a4b4     nt!PnpDeleteLockedDeviceNodes+0xd7**

**16 ffff9900`395ef7b0 fffff802`09161769     nt!PnpProcessQueryRemoveAndEject+0x418**

**17 ffff9900`395ef890 fffff802`09173a40     nt!PnpProcessTargetDeviceEvent+0x109**

**18 ffff9900`395ef8c0 fffff802`08cc1c65     nt!PnpDeviceEventWorker+0x2c0**

**19 ffff9900`395ef940 fffff802`08ce9dc7     nt!ExpWorkerThread+0x155**

**1a ffff9900`395efb30 fffff802`08e421e4     nt!PspSystemThreadStartup+0x57**

**1b ffff9900`395efb80 00000000`00000000     nt!KiStartSystemThread+0x34**

Outstanding IntcBtLE poolusage includes leaked WDFIOTARGET and related object context:

**0: kd> !wdfpoolusage IntcBtLE 0 7**

**-----------------------------------**

**FxDriverGlobals ffffc4883cbe4e00 pool stats**

**-----------------------------------**

**Driver Tag: 'Intc'**

**1208 NonPaged Bytes, 0 Paged Bytes**

**4 NonPaged Allocations, 0 Paged Allocations**

**211203 PeakNonPaged Bytes, 6190 PeakPaged Bytes**

**975 PeakNonPaged Allocations, 47 PeakPaged Allocations**

**Client alloc starts at ffffc48842cfcda0**

**Size  608 Tag 'Intc'**

**NonPagedPoolNx (0x200)**

**!wdfiotarget 0x00003b77bd303228 [ACXTARGETCIRCUIT]**

**dt FxIoTarget 0xffffc48842cfcdd0**

**Caller:  Wdf01000!FxIoTargetRemote::\_Create+13d**

**Client alloc starts at ffffc48842d02f50**

**Size  176 Tag 'Intc'**

**NonPagedPoolNx (0x200)**

**Caller:  Wdf01000!FxNonPagedObject::FxNonPagedObject+47**

**Client alloc starts at ffffc48842d08ec0**

**Size  312 Tag 'Intc'**

**NonPagedPoolNx (0x200)**

**Caller:  Wdf01000!imp\_WdfObjectAllocateContext+7d**

**Client alloc starts at ffffc48842d0cf90**

**Size  112 Tag 'Intc'**

**NonPagedPoolNx (0x200)**

**Caller:  Wdf01000!imp\_WdfObjectAllocateContext+7d**

The leaked WDFIOTARGET was allocated in Acx01000!Acx::AfxManagerCircuitInfo::Init:

**0: kd> !wdfobject 0xffffc48842cfcdd0**

**The type for object 0xffffc48842cfcdd0 is FxIoTarget**

**State: FxObjectStateDeletedAndDisposed (0xa)**

**!wdfhandle 0x00003b77bd303228**

**dt Wdf01000!FxIoTarget 0xffffc48842cfcdd0**

**Contexts:**

**context:  dt 0xffffc48842d08ef0 Acx01000!AfxTargetCircuit (size is 0xd8 bytes)**

**EvtDestroyCallback fffff806d8a04780 Acx01000!Acx::WdfCpp::CxObjectContext<ACXTARGETCIRCUIT\_\_ \* \_\_ptr64,Acx::AfxTargetCircuit>::EvtCxObjectContextDestroyThunk**

**context:  dt 0xffffc48842d0cfc0 Acx01000!WdfCustomType\_ACXTARGETCIRCUIT (size is 0x10 bytes)**

**…**

**Owning device: !wdfdevice 0x00003b77bdbe73c8**

The device is deleted already:

**0: kd> !wdfhandle 0x00003b77bdbe73c8**

**Treating handle as a KMDF handle!**

**Dumping WDFHANDLE 0x00003b77bdbe73c8**

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

**Refcount: 0**

**Contexts:**

**<no associated contexts or attribute callbacks>**

**!wdfobject 0xffffc48842418c30**

**0: kd> !verifier 80 0xffffc48842418c30**

**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 0xffffc48842418c30.**

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

**Pool block ffffc48842418bb0, Size 0000000000000450, Thread ffffc48840b98040**

**fffff802094ee788 nt!VfPtFreePoolNotification+0x5c**

**fffff80208ebac14 nt!ExpFreePoolChecks+0x2164c4**

**fffff802090260c7 nt!ExpFreeHeapSpecialPool+0x5f**

**fffff802094befc3 nt!ExFreePoolWithTag+0x763**

**fffff80208ff0292 nt!DifExFreePoolWithTagWrapper+0xc2**

**fffff8020a1c6ed5 Wdf01000!FxPoolFree+0x39**

**fffff8020a1fdffa Wdf01000!FxDevice::`scalar deleting destructor'+0x2a**

**fffff8020a1c931b Wdf01000!FxObject::SelfDestruct+0x1b**

**fffff8020a1c544f Wdf01000!FxObject::ProcessDestroy+0xaf**

**fffff8020a1c6459 Wdf01000!FxObject::Release+0x49**

**fffff8020a1c351d Wdf01000!FxObject::DeletedAndDisposedWorkerLocked+0x4d**

**fffff8020a1d25cc Wdf01000!FxObject::DeleteObject+0xf30c**

**fffff8020a1fe6b6 Wdf01000!FxDevice::DeleteObject+0x116**

**fffff8020a2328e7 Wdf01000!FxPkgPnp::DeleteDevice+0x23**

**fffff8020a235985 Wdf01000!FxPkgPnp::ProcessDelayedDeletion+0x59**

**fffff8020a22a860 Wdf01000!FxPostProcessInfo::Evaluate+0x58**

**fffff8020a22c817 Wdf01000!FxPkgPnp::PnpProcessEvent+0x1b3**

**fffff8020a1e5c00 Wdf01000!FxChildList::NotifyDeviceRemove+0x1a4**

**fffff8020a22b973 Wdf01000!FxPkgPnp::PnpEventRemoved+0x53**

**fffff8020a22ad27 Wdf01000!FxPkgPnp::PnpEnterNewState+0x15f**

**fffff8020a22c9af Wdf01000!FxPkgPnp::PnpProcessEventInner+0x163**

**fffff8020a22c7e6 Wdf01000!FxPkgPnp::PnpProcessEvent+0x182**

**fffff8020a236c32 Wdf01000!FxPkgPnp::\_PnpRemoveDevice+0xa2**

**fffff8020a1c7a94 Wdf01000!FxPkgPnp::Dispatch+0xd4**

**fffff8020a1c7b41 Wdf01000!FxDevice::DispatchWithLock+0x81**

**fffff80208ca34e5 nt!IofCallDriver+0x55**

**fffff806d9ba149a ksthunk!CKernelFilterDevice::DispatchIrp+0x17a**

**fffff806d9ba1133 ksthunk!CKernelFilterDevice::DispatchIrpBridge+0x13**

**fffff80208ca34e5 nt!IofCallDriver+0x55**

**fffff802091330a4 nt!IopSynchronousCall+0xf8**

**fffff8020923978c nt!IopRemoveDevice+0x108**

**fffff80208db6150 nt!PnpRemoveLockedDeviceNode+0x1a8**

**fffff8020923935a nt!PnpDeleteLockedDeviceNode+0x4e**

**fffff80209239027 nt!PnpDeleteLockedDeviceNodes+0xd7**

**fffff8020923a4b4 nt!PnpProcessQueryRemoveAndEject+0x418**

**fffff80209161769 nt!PnpProcessTargetDeviceEvent+0x109**

**fffff80209173a40 nt!PnpDeviceEventWorker+0x2c0**

**fffff80208cc1c65 nt!ExpWorkerThread+0x155**

**fffff80208ce9dc7 nt!PspSystemThreadStartup+0x57**

**fffff80208e421e4 nt!KiStartSystemThread+0x34**

**Finished parsing all pool tracking information.**

But the WDFIOTARGET object Reference count is non-zero, hence it is not destroyed and considered to be leaked:

**0: kd> dt Wdf01000!FxIoTarget 0xffffc48842cfcdd0 m\_Refcnt**

**+0x00c m\_Refcnt : 0n1**

Acx01000 allocated the object and IntcBtLE has no control over the object’s lifetime.

<https://hsdes.intel.com/appstore/article/#/14019486323>

[GNR XCC A1][2S][Windows][DM] System hit BSOD (CRYPTO\_LIBRARY\_INTERNAL\_ERROR) while running Sandstone on 32 VM's:

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

**CRYPTO\_LIBRARY\_INTERNAL\_ERROR (171)**

**An internal error in the crypto libraries.**

**This BugCheck will hit if the crypto libraries detect an anomaly**

**that should never occur but which might be the symptom of an**

**active attack, and the library has no safe method of signaling**

**the error to the caller.**

**Arguments:**

**Arg1: 0000000072647378, ID of failure.**

**Arg2: 0000000000000000, Reserved.**

**Arg3: 0000000000000000, Reserved.**

**Arg4: 0000000000000000, Reserved.**

**12: kd> k**

**# Child-SP          RetAddr               Call Site**

**00 fffff303`e5bd70b8 fffff807`6033de12     nt!KeBugCheckEx**

**01 (Inline Function) --------`--------     cng!SymCryptFatalEnvWindowsKernelmodeWin8\_1nLater+0x1a**

**02 (Inline Function) --------`--------     cng!SymCryptFatal+0x1a**

**03 (Inline Function) --------`--------     cng!SymCryptRdseedGet+0x36bd7**

**04 fffff303`e5bd70c0 fffff807`60309bf9     cng!RdrandPushEntropy+0x36cd2**

**05 fffff303`e5bd7190 fffff807`602f764c     cng!RdrandCallback+0x9**

**06 fffff303`e5bd71c0 fffff807`602f7572     cng!EntropyPerformCallbacks+0xa8**

**07 fffff303`e5bd7200 fffff807`5c9636ee     cng!reseedWorkItemRoutine+0x12**

**08 fffff303`e5bd7230 fffff807`5c919111     nt!IopProcessWorkItem+0x8e**

**09 fffff303`e5bd72a0 fffff807`5c8c8785     nt!ExpWorkerThread+0x161**

**0a fffff303`e5bd74b0 fffff807`5ca1ed48     nt!PspSystemThreadStartup+0x55**

**0b fffff303`e5bd7500 00000000`00000000     nt!KiStartSystemThread+0x28**

<https://hsdes.intel.com/appstore/article/#/14019445133>

[MTLH][RVP][S4] Break observed during 5 S4 Cycles (MEMORY\_CORRUPTION\_LARGE):

**12: 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: ffff94858fc09e88, name of the driver having the issue.**

**Arg3: ffff94858ac369d0, verifier internal structure with driver information.**

**Arg4: 0000000000000001, 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.**

**12: kd> du ffff94858fc09e88**

**ffff9485`8fc09e88  "ibtusb.sys"**

**12: kd> !verifier 3 ibtusb.sys**

**Verify Flags Level 0x001209bb**

**STANDARD FLAGS:**

**[X] (0x00000000) Automatic Checks**

**[X] (0x00000001) Special pool**

**[X] (0x00000002) Force IRQL checking**

**[X] (0x00000008) Pool tracking**

**[X] (0x00000010) I/O verification**

**[X] (0x00000020) Deadlock detection**

**[X] (0x00000080) DMA checking**

**[X] (0x00000100) Security checks**

**[X] (0x00000800) Miscellaneous checks**

**[X] (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     0x223e**

**Synch Executions     0x1a35**

**Trims                0x4baa**

**Pool Allocations Attempted             0x7a162**

**Pool Allocations Succeeded             0x7a162**

**Pool Allocations Succeeded SpecialPool 0x7a162**

**Pool Allocations With NO TAG           0x0**

**Pool Allocations Failed                0x0**

**Current paged pool allocations         0x22f for 000110FF bytes**

**Peak paged pool allocations            0x27f for 04B3DD38 bytes**

**Current nonpaged pool allocations      0x76c8 for 0293484F bytes**

**Peak nonpaged pool allocations         0x78b0 for 02A5D8D1 bytes**

**Driver Verification List**

**------------------------**

**nt!\_VF\_TARGET\_DRIVER 0xffff94858c0704b0: ibtusb.sys (Loaded and Unloaded)**

**Pool Allocation Statistics: ( NonPagedPool / PagedPool )**

**Current Pool Allocations: ( 0x00000001 / 0x00000000 )**

**Current Pool Bytes:       ( 0x00000050 / 0x00000000 )**

**Peak Pool Allocations:    ( 0x00000003 / 0x00000000 )**

**Peak Pool Bytes:          ( 0x0000051b / 0x00000000 )**

**Contiguous Memory Bytes:       0x00000000**

**Peak Contiguous Memory Bytes:  0x00000000**

**Pool Allocations:**

**Address             Length      Tag   Caller Address**

**------------------  ----------  ----  ------------------**

**0xffff9485b6a0cfb0  0x00000050  0VWF  0xfffff80115cc8efd  ibtusb!ExAllocatePoolZero+0x2d**

<https://hsdes.intel.com/appstore/article/#/14020741426>

[Windows Server 2022 Servicing ] Request to backport GHESv2 bug fix to Windows Server 2022:

kd> !analyze -v

PAGE\_FAULT\_IN\_NONPAGED\_AREA (50)

Invalid system memory was referenced.  This cannot be protected by try-except.

Typically the address is just plain bad or it is pointing at freed memory.

Arguments:

Arg1: ffffe505a5200018, memory referenced.

Arg2: 0000000000000002, X64: bit 0 set if the fault was due to a not-present PTE.

bit 1 is set if the fault was due to a write, clear if a read.

bit 3 is set if the processor decided the fault was due to a corrupted PTE.

bit 4 is set if the fault was due to attempted execute of a no-execute PTE.

- ARM64: bit 1 is set if the fault was due to a write, clear if a read.

bit 3 is set if the fault was due to attempted execute of a no-execute PTE.

Arg3: fffff801237b9869, If non-zero, the instruction address which referenced the bad memory

address.

Arg4: 0000000000000002, (reserved)

PROCESS\_NAME:  System

TRAP\_FRAME:  ffff818ad9a07050 -- (.trap 0xffff818ad9a07050)

NOTE: The trap frame does not contain all registers.

Some register values may be zeroed or incorrect.

rax=0000000000000300 rbx=0000000000000000 rcx=000000008db42400

rdx=0000000000abfffe rsi=0000000000000000 rdi=0000000000000000

rip=fffff801237b9869 rsp=ffff818ad9a071e8 rbp=ffffe50574c00000

 r8=ffffe5056b6a3870  r9=ffffe505a5200018 r10=00000000d49a1d98

r11=ffffe50574c00000 r12=0000000000000000 r13=0000000000000000

r14=0000000000000000 r15=0000000000000000

iopl=0         nv up ei pl nz na pe cy

nt!WheapInitializeErrorRecordWrapper+0x59:

fffff801`237b9869 458911          mov     dword ptr [r9],r10d ds:ffffe505`a5200018=????????

Resetting default scope

STACK\_TEXT:

ffff818a`d9a06da8 fffff801`23659dc7     : 00000000`00000050 ffffe505`a5200018 00000000`00000002 ffff818a`d9a07050 : nt!KeBugCheckEx

ffff818a`d9a06db0 fffff801`236add4e     : ffffffff`ffffffff 00000000`00000002 00000000`00000000 ffffe505`a5200018 : nt!MiSystemFault+0xa07

ffff818a`d9a06eb0 fffff801`2382ff41     : 00000000`0001e2d0 fffff801`23676bb5 00000000`00000001 ffff818a`d9a07141 : nt!MmAccessFault+0x2ee

ffff818a`d9a07050 fffff801`237b9869     : fffff801`23c0dd69 ffffe505`6b6a3870 00000000`61656857 00000000`c46e70a8 : nt!KiPageFault+0x341

ffff818a`d9a071e8 fffff801`23c0dd69     : ffffe505`6b6a3870 00000000`61656857 00000000`c46e70a8 00000000`00000000 : nt!WheapInitializeErrorRecordWrapper+0x59

ffff818a`d9a071f0 fffff801`23eda218     : ffffe505`6b6a3870 00000000`00000008 00000000`00000000 00000000`00000000 : nt!WheapInitializeErrorSource+0xb5

ffff818a`d9a07230 fffff801`23eda6ce     : ffffe505`5c0bb040 ffff818a`d9a072c8 ffffe505`5c0bb6e0 00000000`00000001 : nt!WheapInitializeErrorSourceTable+0x110

ffff818a`d9a07260 fffff801`23ed9e67     : fffff801`1ebd6c50 fffff801`00000009 00000000`00000000 00000000`00000000 : nt!WheaInitialize+0x45a

ffff818a`d9a07310 fffff801`23f00515     : fffff801`20eb8000 fffff801`1ebd6c50 fffff801`23c3c480 fffff801`1ebd6c00 : nt!IoInitSystemPreDrivers+0xcf3

ffff818a`d9a07450 fffff801`23c3c4bb     : fffff801`1ebd6c50 fffff801`24052668 fffff801`23c3c480 fffff801`1ebd6c50 : nt!IoInitSystem+0x15

ffff818a`d9a07480 fffff801`23769f15     : ffffe505`5c0bb040 fffff801`23c3c480 fffff801`1ebd6c50 0680ae67`ff3ef567 : nt!Phase1Initialization+0x3b

ffff818a`d9a074b0 fffff801`23824488     : fffff801`20e68180 ffffe505`5c0bb040 fffff801`23769ec0 fef96950`90faa31e : nt!PspSystemThreadStartup+0x55

ffff818a`d9a07500 00000000`00000000     : ffff818a`d9a08000 ffff818a`d9a01000 00000000`00000000 00000000`00000000 : nt!KiStartSystemThread+0x28

SYMBOL\_NAME:  nt!WheapInitializeErrorRecordWrapper+59

MODULE\_NAME: nt

IMAGE\_NAME:  ntkrnlmp.exe

IMAGE\_VERSION:  10.0.20348.1906

<https://hsdes.intel.com/appstore/article/#/22018984996>

[LNL][RVP][APP VRF] With appverifier enabled, SUT immediately breaks due to igfxEMN.exe:

**5: kd> !analyze -v**

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

**\*                                                                             \***

**\*                        Bugcheck Analysis                                    \***

**\*                                                                             \***

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

**…**

**Debugging Details:**

**------------------**

**APPLICATION\_VERIFIER\_LEAK\_REGISTRY (902)**

**An HKEY was leaked.**

**This stop is generated if the owner dll of the registry key was dynamically**

**unloaded while owning resources.**

**Arguments:**

**Arg1: 0000000000000014, Value of the leaked HKEY.**

**Arg2: 000001a564ccee30, Address to the allocation stack trace. Run dps <address> to view the allocation stack.**

**Arg3: 000001a56fd26fe4, Address of the owner dll name. Run du <address> to read the dll name.**

**Arg4: 00007ffb85a00000, Base of the owner dll. Run .reload <dll\_name> = <address> to reload the owner dll. Use 'lm' to get more information about the loaded and unloaded modules.**

**…**

**5: kd> du 000001a56fd26fe4**

**000001a5`6fd26fe4  "igfxLHM.dll"**

**5: kd> !handle 0000000000000014**

**PROCESS ffff8b0fd43a3080**

**SessionId: none  Cid: 1f50    Peb: 93bd41000  ParentCid: 0f08**

**DirBase: 1d1875000  ObjectTable: ffffad8b00e05c40  HandleCount: 165.**

**Image: igfxEMN.exe**

**Handle table at ffffad8b00e05c40 with 165 entries in use**

**0014: Object: ffffad8b00756780  GrantedAccess: 00020019 (Protected) (Audit) Entry: ffffad8afab31050**

**Object: ffffad8b00756780  Type: (ffff8b0fc0da6bc0) Key**

**ObjectHeader: ffffad8b00756750 (new version)**

**HandleCount: 1  PointerCount: 32767**

**Directory Object: 00000000  Name: \REGISTRY\MACHINE\SYSTEM\CONTROLSET001\CONTROL\CLASS\{5C4C3332-344D-483C-8739-259E934C9CC8}\0007**

**5: kd> dps 000001a564ccee30**

**000001a5`64ccee30  000001a5`64c8e930**

**000001a5`64ccee38  001c0000`0000f801**

**000001a5`64ccee40  00007ffb`85a08135 igfxLHM!GetHKRHandleForExtensionINF+0xc9**

**000001a5`64ccee48  00007ffb`85a09ba2 igfxLHM!CCUIString::LoadCustomizedString+0x36**

**000001a5`64ccee50  00007ffb`85a04f8a igfxLHM!CCUIString::LoadStringResource+0x2a**

**000001a5`64ccee58  00007ffb`85d5f781 igfxDHN!igfxLHMLib::ICUIString::LoadStringResource+0x4d**

**000001a5`64ccee60  00007ffb`85d5f3fe igfxDHN!CDataHandler::InitializePresetProfileStrings+0x86**

**000001a5`64ccee68  00007ffb`85d5f54b igfxDHN!CDataHandler::InitializeProfiles+0x1f**

**000001a5`64ccee70  00007ffb`85d5e74e igfxDHN!CDataHandler::CDataHandler+0x266**

**000001a5`64ccee78  00007ffb`85d55e49 igfxDHN!ATL::CComCreator<ATL::CComObject<CDataHandler> >::CreateInstance+0x65**

**000001a5`64ccee80  00007ffb`85d558f8 igfxDHN!ATL::CComClassFactory::CreateInstance+0x58**

**000001a5`64ccee88  00007ffb`b73edae2 combase!CServerContextActivator::CreateInstance+0x202**

**000001a5`64ccee90  00007ffb`b73e4996 combase!ActivationPropertiesIn::DelegateCreateInstance+0x196**

**000001a5`64ccee98  00007ffb`b74baa87 combase!CApartmentActivator::CreateInstance+0xa7**

**000001a5`64cceea0  00007ffb`b73e45a7 combase!CProcessActivator::CCICallback+0x57**

**000001a5`64cceea8  00007ffb`b74bd0bd combase!CProcessActivator::AttemptActivation+0x8d**

**5: kd> k**

**# Child-SP          RetAddr               Call Site**

**00 00000009`3befeb70 00007ffb`a671824e     vrfcore!VerifierStopMessageEx+0x827**

**01 00000009`3befeec0 00007ffb`a6718cdf     vfbasics!AVrfpCheckDllLeaks+0xda**

**02 00000009`3befef20 00007ffb`b80ec407     vfbasics!AVrfLeakDllUnload+0xa7**

**03 00000009`3beff370 00007ffb`b80cb1a0     ntdll!AVrfDllUnloadNotification+0x9b**

**04 00000009`3beff3b0 00007ffb`b8044f77     ntdll!LdrpUnloadNode+0xaf778**

**05 00000009`3beff400 00007ffb`b8044eea     ntdll!LdrpDecrementModuleLoadCountEx+0x77**

**06 (Inline Function) --------`--------     ntdll!LdrpDecrementModuleLoadCount+0xf**

**07 00000009`3beff430 00007ffb`b5962aee     ntdll!LdrUnloadDll+0x9a**

**08 00000009`3beff460 00007ffb`b73fe02e     KERNELBASE!FreeLibrary+0x1e**

**09 00000009`3beff490 00007ffb`b73ff21d     combase!CClassCache::CDllPathEntry::CFinishObject::Finish+0x2e**

**0a 00000009`3beff4c0 00007ffb`b73fee75     combase!CClassCache::CFinishComposite::Finish+0x55**

**0b 00000009`3beff4f0 00007ffb`b73fec62     combase!CClassCache::CleanUpDllsForApartment+0x1f1**

**0c (Inline Function) --------`--------     combase!CCCleanUpDllsForApartment+0xe**

**0d (Inline Function) --------`--------     combase!FinishShutdown::\_\_l2::<lambda\_ac39365968346bea08de70a73a47183a>::operator()+0xe**

**0e 00000009`3beff690 00007ffb`b73fffe1     combase!ObjectMethodExceptionHandlingAction<<lambda\_ac39365968346bea08de70a73a47183a> >+0x12**

**0f 00000009`3beff6e0 00007ffb`b74010ab     combase!FinishShutdown+0x55**

**10 00000009`3beff710 00007ffb`b7400a8b     combase!ApartmentUninitialize+0xc3**

**11 00000009`3beff7b0 00007ffb`b7400515     combase!wCoUninitialize+0x35f**

**12 00000009`3beff800 00007ffb`a671e1bf     combase!CoUninitialize+0x165**

**13 00000009`3beff8f0 00007ff6`a8bed1ff     vfbasics!AVrfpCoUninitialize+0x1f**

**14 00000009`3beff940 00007ff6`a8bf2c1a     igfxEMN!IsIntelFamily+0x97**

**15 00000009`3beff990 00007ff6`a8c08e02     igfxEMN!wWinMain+0x3e**

**16 (Inline Function) --------`--------     igfxEMN!invoke\_main+0x21**

**17 00000009`3beff9c0 00007ffb`b6f41f87     igfxEMN!\_\_scrt\_common\_main\_seh+0x106**

**18 00000009`3beffa00 00007ffb`b8078ef0     KERNEL32!BaseThreadInitThunk+0x17**

**19 00000009`3beffa30 00000000`00000000     ntdll!RtlUserThreadStart+0x20**

<https://hsdes.intel.com/appstore/article/#/22018974063>

[LNL-M] [RVP] KMODE\_EXCEPTION\_NOT\_HANDLED (1e) appid.sys:

0: kd> !analyze -v

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

\*                                                                             \*

\*                        Bugcheck Analysis                                    \*

\*                                                                             \*

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

KMODE\_EXCEPTION\_NOT\_HANDLED (1e)

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: fffff80443c761d1, The address that the exception occurred at

Arg3: 0000000000000000, Parameter 0 of the exception

Arg4: 0000000000000028, Parameter 1 of the exception

Debugging Details:

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

KEY\_VALUES\_STRING: 1

    Key  : Analysis.CPU.mSec

    Value: 3842

    Key  : Analysis.DebugAnalysisManager

    Value: Create

    Key  : Analysis.Elapsed.mSec

    Value: 8344

    Key  : Analysis.Init.CPU.mSec

    Value: 2217

    Key  : Analysis.Init.Elapsed.mSec

    Value: 20350

    Key  : Analysis.Memory.CommitPeak.Mb

    Value: 163

    Key  : WER.OS.Branch

    Value: rs\_prerelease

    Key  : WER.OS.Timestamp

    Value: 2023-10-06T14:24:00Z

    Key  : WER.OS.Version

    Value: 10.0.25972.1000

FILE\_IN\_CAB:  MEMORY.DMP

TAG\_NOT\_DEFINED\_202b:  \*\*\* Unknown TAG in analysis list 202b

DUMP\_FILE\_ATTRIBUTES: 0x1800

BUGCHECK\_CODE:  1e

BUGCHECK\_P1: ffffffffc0000005

BUGCHECK\_P2: fffff80443c761d1

BUGCHECK\_P3: 0

BUGCHECK\_P4: 28

BLACKBOXACPI: 1 (!blackboxacpi)

BLACKBOXBSD: 1 (!blackboxbsd)

BLACKBOXNTFS: 1 (!blackboxntfs)

BLACKBOXPNP: 1 (!blackboxpnp)

BLACKBOXWINLOGON: 1

PROCESS\_NAME:  IntelAudioService.exe

TRAP\_FRAME:  ffffb98360f71e80 -- (.trap 0xffffb98360f71e80)

NOTE: The trap frame does not contain all registers.

Some register values may be zeroed or incorrect.

rax=0000000000000012 rbx=0000000000000000 rcx=ffffb98360f72248

rdx=0000000000020019 rsi=0000000000000000 rdi=0000000000000000

rip=fffff80443c761d1 rsp=ffffb98360f72010 rbp=ffffb98360f72090

 r8=ffffb98360f721d0  r9=ffffb98360f72248 r10=fffff804438da6d0

r11=00000000071b5000 r12=0000000000000000 r13=0000000000000000

r14=0000000000000000 r15=0000000000000000

iopl=0         nv up ei ng nz ac pe cy

nt!KiSystemServiceRepeat+0x3d:

fffff804`43c761d1 498bc3          mov     rax,r11

Resetting default scope

STACK\_TEXT:

ffffb983`60f715b8 fffff804`43ccf2f1     : 00000000`0000001e ffffffff`c0000005 fffff804`43c761d1 00000000`00000000 : nt!KeBugCheckEx

ffffb983`60f715c0 fffff804`43c76d85     : 00000000`00000000 00000000`00000000 00000000`00000000 fffff804`43b72ed5 : nt!KiDispatchException+0x181a01

ffffb983`60f71ca0 fffff804`43c72002     : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : nt!KiExceptionDispatch+0x145

ffffb983`60f71e80 fffff804`43c761d1     : 00000000`00000001 ffff8689`c42e6cc0 00000000`00000000 ffffb983`60f722b0 : nt!KiPageFault+0x442

ffffb983`60f72010 fffff804`43c64d80     : fffff804`635c6426 ffffcc84`dd0d8690 00000000`c0000034 ffffb983`60f722b0 : nt!KiSystemServiceRepeat+0x3d

ffffb983`60f721a8 fffff804`635c6426     : ffffcc84`dd0d8690 00000000`c0000034 ffffb983`60f722b0 ffffb983`60f72280 : nt!KiServiceLinkage

ffffb983`60f721b0 fffff804`63594c4b     : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : appid!AiRegOpenKey+0x4a

ffffb983`60f72210 fffff804`635b9ae0     : 00000000`00000000 ffffb983`60f722a0 00000000`00000001 00000000`00000000 : appid!AiRegReadQwordValue+0x37

ffffb983`60f72260 fffff804`635bb2d5     : 00000000`00000000 ffffcc84`db2ebc58 00000000`00000000 00000000`00000000 : appid!SmartlockerSmartScreenRegistryIsEnabled+0x4c

ffffb983`60f722b0 fffff804`635bbd93     : 00000000`1da74201 ffffcc84`00000000 00000000`1da74201 ffffcc84`db2ebc58 : appid!SrpIsOnlySmartAppControlEnabledForPolicyType+0x5d

ffffb983`60f72320 fffff804`635b74fb     : 00000000`00000000 00000000`00225804 00000000`00000fff ffff8689`ba4b3010 : appid!SrpVerifyDll+0x3ab

ffffb983`60f724d0 fffff804`43a62625     : 00000000`42536f49 00000000`00000069 00000000`00060070 fffff804`442c841c : appid!AipDeviceIoControlDispatch+0x5db

ffffb983`60f725b0 fffff804`43eb63b6     : ffff8689`c2302e10 ffff8689`c4046310 ffff8689`c3294700 00000000`00000000 : nt!IofCallDriver+0x65

ffffb983`60f725f0 fffff804`43eb5117     : 00000000`00000005 ffff8689`c3294700 00000000`00000000 ffff8689`c3294700 : nt!IopSynchronousServiceTail+0x476

ffffb983`60f726a0 fffff804`43eb49be     : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : nt!IopXxxControlFile+0x747

ffffb983`60f72940 fffff804`43c76315     : 00000000`7ffe0384 00000000`7ffe0385 00000000`0000000c 0000003e`1e3fdd10 : nt!NtDeviceIoControlFile+0x5e

ffffb983`60f729b0 00007ff9`c3356864     : 00007ff9`c3328368 00000000`000000e4 0000003e`1e3fdd10 00000000`00000000 : nt!KiSystemServiceCopyEnd+0x25

0000003e`1e3fdab8 00007ff9`c3328368     : 00000000`000000e4 0000003e`1e3fdd10 00000000`00000000 00000000`00000000 : ntdll!NtDeviceIoControlFile+0x14

0000003e`1e3fdac0 00007ff9`c3328145     : 0000003e`1e3fdd10 00000000`00000000 00000000`00000000 00000000`000004fc : ntdll!SaferpIsDllAllowed+0x12c

0000003e`1e3fdb90 00007ff9`c331d5b0     : 00000000`00000000 0000003e`1e3fdd10 0000003e`00000001 00000000`00000000 : ntdll!LdrpCodeAuthzCheckDllAllowedSrpV2+0x35

0000003e`1e3fdbc0 00007ff9`c331ce81     : 00000000`00000000 0000003e`1e3fdd10 0000023b`4e35a3c8 0000023b`00000000 : ntdll!LdrpMapDllNtFileName+0x1d8

0000003e`1e3fdcd0 00007ff9`c331cc2f     : 00000000`00000000 0000023b`353fea50 00000000`00000001 0000003e`1e3fe130 : ntdll!LdrpMapDllFullPath+0xf5

0000003e`1e3fde60 00007ff9`c32e8b50     : 0000023b`353fea50 0000003e`1e3fe001 0000003e`1e3fdf98 00000000`00000000 : ntdll!LdrpProcessWork+0x87

0000003e`1e3fdeb0 00007ff9`c32cc06a     : 0000003e`1e3fdfa0 0000003e`1e3fe140 0000003e`1e3fe130 00670067`006f0000 : ntdll!LdrpLoadDllInternal+0x204

0000003e`1e3fdf40 00007ff9`c32e869e     : 00000000`00000000 00000000`00000009 00000000`00000080 00000000`00000000 : ntdll!LdrpLoadDll+0xc2

0000003e`1e3fe100 00007ff9`c08434c2     : 00000000`00000000 00000000`00000008 00000000`000000de 00000000`00000000 : ntdll!LdrLoadDll+0x14e

0000003e`1e3fe200 00007ff9`a43c0b4c     : 0000003e`00000000 00000000`00008001 00000000`00000000 00000000`00000000 : KERNELBASE!LoadLibraryExW+0x172

0000003e`1e3fe270 00000000`00000000     : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : clr!CLRLoadLibraryExWorker+0x4c

SYMBOL\_NAME:  appid!AiRegOpenKey+4a

MODULE\_NAME: appid

IMAGE\_NAME:  appid.sys

STACK\_COMMAND:  .cxr; .ecxr ; kb

BUCKET\_ID\_FUNC\_OFFSET:  4a

FAILURE\_BUCKET\_ID:  AV\_appid!AiRegOpenKey

OS\_VERSION:  10.0.25972.1000

BUILDLAB\_STR:  rs\_prerelease

OSPLATFORM\_TYPE:  x64

OSNAME:  Windows 10

FAILURE\_ID\_HASH:  {0daaf693-27d2-cea5-df20-89a65282e557}

Followup:     MachineOwner

<https://hsdes.intel.com/appstore/article/#/22018973022>

[MTL-P] [RVP] NDIS\_BUGCHECK\_MINIPORT\_FATAL\_ERROR (15e) Netwtw12.sys:

Microsoft (R) Windows Debugger Version 10.0.22621.755 AMD64

Copyright (c) Microsoft Corporation. All rights reserved.

Loading Dump File [C:\DMP\10.16\NDIS-20231013-1257.dmp]

Kernel Bitmap Dump File: Kernel address space is available, User address space may not be available.

Symbol search path is: srv\*

Executable search path is:

Windows 10 Kernel Version 25972 MP (22 procs) Free x64

Product: WinNt, suite: TerminalServer SingleUserTS

Edition build lab: 25972.1000.amd64fre.rs\_prerelease.231006-1424

Machine Name:

Kernel base = 0xfffff806`62e00000 PsLoadedModuleList = 0xfffff806`63a13df0

Debug session time: Fri Oct 13 12:57:38.919 2023 (UTC - 7:00)

System Uptime: 0 days 0:18:10.645

Loading Kernel Symbols

...............................................................

................................................................

................................................................

...................................

Loading User Symbols

Loading unloaded module list

..................

For analysis of this file, run !analyze -v

0: kd> !symfix

0: kd> !reload

Loading Kernel Symbols

...............................................................

................................................................

................................................................

...................................

Loading User Symbols

Loading unloaded module list

..................

0: kd> !analyze -v

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

\*                                                                             \*

\*                        Bugcheck Analysis                                    \*

\*                                                                             \*

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

BUGCODE\_NDIS\_DRIVER\_LIVE\_DUMP (15e)

The operating system recovered from an error in a networking driver.

NDIS has detected and recovered from a serious problem in another network

driver. Although the system was not halted, this problem may later cause

connectivity problems or a fatal BugCheck.

Arguments:

Arg1: 0000000000000001, NDIS\_BUGCHECK\_MINIPORT\_FATAL\_ERROR

A miniport has encountered a fatal error and requested

re-enumeration.

Arg2: ffffda8e6fc941a0, A pointer to Miniport block. !ndiskd.miniport on

this pointer for more info.

Arg3: ffffda8e514a5360, A pointer to the Miniport's PDO

Arg4: 0000000000000047, The fatal error that caused this live dump to be taken

Debugging Details:

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

Unable to load image \SystemRoot\System32\DriverStore\FileRepository\netwtw6e.inf\_amd64\_71f8441d5224dfab\Netwtw12.sys, Win32 error 0n2

KEY\_VALUES\_STRING: 1

    Key  : Analysis.CPU.mSec

    Value: 4936

    Key  : Analysis.DebugAnalysisManager

    Value: Create

    Key  : Analysis.Elapsed.mSec

    Value: 5931

    Key  : Analysis.Init.CPU.mSec

    Value: 3796

    Key  : Analysis.Init.Elapsed.mSec

    Value: 51541

    Key  : Analysis.Memory.CommitPeak.Mb

    Value: 110

    Key  : WER.OS.Branch

    Value: rs\_prerelease

    Key  : WER.OS.Timestamp

    Value: 2023-10-06T14:24:00Z

    Key  : WER.OS.Version

    Value: 10.0.25972.1000

FILE\_IN\_CAB:  NDIS-20231013-1257.dmp

DUMP\_FILE\_ATTRIBUTES: 0x810

  Live Generated Dump

BUGCHECK\_CODE:  15e

BUGCHECK\_P1: 1

BUGCHECK\_P2: ffffda8e6fc941a0

BUGCHECK\_P3: ffffda8e514a5360

BUGCHECK\_P4: 47

DRIVER\_OBJECT: ffffda8e735827b0

FAULTING\_MODULE: fffff80687600000 Netwtw12

PROCESS\_NAME:  System

STACK\_TEXT:

fffffd0f`8e9a7230 fffff806`6300cee2     : 00000000`00000000 fffffd0f`8e9a7300 ffffda8e`76d05240 00000000`00000000 : nt!IopLiveDumpCollectPages+0x90

fffffd0f`8e9a7280 fffff806`638a2696     : 00000000`00000000 ffffda8e`76d05240 fffffd0f`8e9a7300 ffffda8e`76d05240 : nt!IopLiveDumpEndMirroringCallback+0x52

fffffd0f`8e9a72b0 fffff806`630102e1     : 00000000`00000000 fffff806`6300e200 ffffda8e`76315010 fffffd0f`8e9a74a0 : nt!MmDuplicateMemory+0x2de

fffffd0f`8e9a7340 fffff806`6300d510     : 00000000`00000000 fffff806`63264d80 ffffda8e`75918720 00000000`00000000 : nt!IopLiveDumpCapture+0x69

fffffd0f`8e9a73a0 fffff806`6300e626     : ffffda8e`76315010 ffffda8e`76315010 ffffa805`0170b428 00000000`00000000 : nt!IopLiveDumpCaptureMemoryPages+0x50

fffffd0f`8e9a74e0 fffff806`63774aa4     : 00000000`00000000 ffffda8e`74f23990 00000000`00000038 ffffa804`fc2b7620 : nt!IoCaptureLiveDump+0x30a

fffffd0f`8e9a7710 fffff806`63775028     : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : nt!DbgkpWerCaptureLiveFullDump+0x180

fffffd0f`8e9a7770 fffff806`6376c298     : fffffd0f`8e9a77b0 00000000`00000000 00000000`00000000 00000000`00000000 : nt!DbgkpWerProcessPolicyResult+0x30

fffffd0f`8e9a77a0 fffff806`636b4c69     : ffffda8e`6fc94200 00000000`00000000 00000002`89fcdde8 ffffda8e`746bc010 : nt!DbgkWerCaptureLiveKernelDump2+0xb7618

fffffd0f`8e9a7800 fffff806`689d8939     : ffffda8e`6fc94200 ffffda8e`4bcc8250 ffffda8e`4bcc8250 ffffda8e`6fc941a0 : nt!DbgkWerCaptureLiveKernelDump+0x69

fffffd0f`8e9a7880 fffff806`68a985d8     : fffffd0f`00000000 ffffda8e`6fc941a0 fffffd0f`8e9a7a50 fffff806`631b06b3 : ndis!ndisMReenumerateFailedAdapterInternal+0x15d

fffffd0f`8e9a78f0 fffff806`6897c691     : ffffda8e`76d05240 00000000`00000000 fffff806`63ba4c00 ffffda8e`4bcc8250 : ndis!ndisQueuedReenumerateFailedAdapter+0x18

fffffd0f`8e9a7920 fffff806`630d7aa5     : ffffda8e`4bcc8250 ffffda8e`76d05240 fffff806`63ba4c00 fffffd0f`8e9a7a50 : ndis!ndisWorkItemHandler+0x11

fffffd0f`8e9a7950 fffff806`631b01d3     : ffffda8e`76d05240 ffffda8e`6ac18dd0 ffffda8e`76d05240 fffff806`630d7950 : nt!ExpWorkerThread+0x155

fffffd0f`8e9a7b30 fffff806`63264414     : ffff8281`e280d180 ffffda8e`76d05240 fffff806`631b0180 00000000`00000000 : nt!PspSystemThreadStartup+0x53

fffffd0f`8e9a7b80 00000000`00000000     : fffffd0f`8e9a8000 fffffd0f`8e9a1000 00000000`00000000 00000000`00000000 : nt!KiStartSystemThread+0x34

CHKIMG\_EXTENSION: !chkimg -lo 50 -d !nt

    fffff80662f506c0-fffff80662f506c2  3 bytes - nt!\_guard\_check\_icall\_fptr

[ 20 4f 13:c0 bf 26 ]

    fffff80662f506c8-fffff80662f506ca  3 bytes - nt!\_guard\_dispatch\_icall\_fptr (+0x08)

[ 70 e2 25:10 c0 26 ]

    fffff80663000165 - nt!RtlCompressBufferXpressHuffStandard+e5

[ 7d:86 ]

    fffff806630008b6 - nt!XpressBuildHuffmanEncodings+26 (+0x751)

[ 76:7f ]

    fffff806630008ca - nt!XpressBuildHuffmanEncodings+3a (+0x14)

[ 75:7e ]

    fffff806630008e8 - nt!XpressBuildHuffmanEncodings+58 (+0x1e)

[ 75:7e ]

    fffff8066300094d - nt!XpressBuildHuffmanEncodings+bd (+0x65)

[ 75:7e ]

    fffff80663000fec - nt!LZ4\_compress\_fast\_extState+4c (+0x69f)

[ 6e:77 ]

    fffff8066300143f - nt!LZ4\_compress\_fast\_extState+49f (+0x453)

[ 6a:73 ]

    fffff80663001474 - nt!LZ4\_compress\_fast\_extState+4d4 (+0x35)

[ 6a:73 ]

    fffff80663001e50 - nt!B\_TREE<\_SM\_PAGE\_KEY,SMKM\_STORE\_MGR<SM\_TRAITS>::SMKM\_FRONTEND\_ENTRY,4096,B\_TREE\_DUMMY\_NODE\_POOL,B\_TREE\_KEY\_COMPARATOR<\_SM\_PAGE\_KEY> >::BTreeNewNode+3c (+0x9dc)

[ 60:69 ]

    fffff80663001eba - nt!ST\_STORE<SM\_TRAITS>::StCompactionPickPriority+42 (+0x6a)

[ 60:69 ]

    fffff806630024f5 - nt!ST\_STORE<SM\_TRAITS>::StCompactionPerformInMem+49 (+0x63b)

[ 59:62 ]

    fffff80663003b02 - nt!SMKM\_STORE\_MGR<SM\_TRAITS>::SmFeAddComplete+46 (+0x160d)

[ 43:4c ]

    fffff80663003ef8 - nt!SMKM\_STORE\_MGR<SM\_TRAITS>::SmFeEvictComplete+48 (+0x3f6)

[ 3f:48 ]

    fffff80663004e54 - nt!ST\_STORE<SM\_TRAITS>::StCompactRegions+54 (+0xf5c)

[ 30:39 ]

    fffff8066300a039 - nt!SmBinaryArrayGrow+89 (+0x51e5)

[ de:e7 ]

    fffff8066300a2d6 - nt!B\_TREE<unsigned long,ST\_STORE<SM\_TRAITS>::\_ST\_HASH\_ENTRY,4096,NP\_CONTEXT,ST\_STORE<SM\_TRAITS>::ST\_HASH\_ENTRY\_COMPARATOR>::BTreeNewNode+3e (+0x29d)

[ db:e4 ]

    fffff8066300ad57 - nt!SmArrayGrow+7b (+0xa81)

[ d1:da ]

    fffff8066300af12 - nt!IoFillDumpHeader+11e (+0x1bb)

[ cf:d8 ]

    fffff8066300af26 - nt!IoFillDumpHeader+132 (+0x14)

[ cf:d8 ]

    fffff8066300c41b - nt!MiMapMemoryDumpMdl+43 (+0x14f5)

[ ba:c3 ]

    fffff8066300c456 - nt!MiMapMemoryDumpMdl+7e (+0x3b)

[ f6:fb ]

    fffff8066300c542 - nt!MiMapMemoryDumpMdl+16a (+0xec)

[ f6:fb ]

    fffff8066300c569-fffff8066300c56a  2 bytes - nt!MiMapMemoryDumpMdl+191 (+0x27)

[ 00 de:80 ba ]

    fffff8066300cc75 - nt!MmFreeIndependentPages+65 (+0x70c)

[ f6:fb ]

    fffff8066300ccb6-fffff8066300ccb7  2 bytes - nt!MmFreeIndependentPages+a6 (+0x41)

[ 00 de:80 ba ]

    fffff8066300cdb6-fffff8066300cdb7  2 bytes - nt!MmFreeIndependentPages+1a6 (+0x100)

[ 00 de:80 ba ]

    fffff8066300d02e - nt!IopLiveDumpCollectPages+b6 (+0x278)

[ ae:b7 ]

    fffff8066300d30e - nt!IopLiveDumpEstimateMemoryPages+fa (+0x2e0)

[ ab:b4 ]

    fffff8066300d337 - nt!IopLiveDumpEstimateMemoryPages+123 (+0x29)

[ ab:b4 ]

    fffff8066300d360 - nt!IopLiveDumpEstimateMemoryPages+14c (+0x29)

[ ab:b4 ]

    fffff8066300d970 - nt!IopLiveDumpAllocAndInitResources+1e4 (+0x610)

[ a5:ae ]

    fffff8066300ea81-fffff8066300ea82  2 bytes - nt!MiFilterCrashDumpPte+81 (+0x1111)

[ 00 de:80 ba ]

    fffff8066300ea9e-fffff8066300ea9f  2 bytes - nt!MiFilterCrashDumpPte+9e (+0x1d)

[ 00 de:80 ba ]

    fffff8066300eabd - nt!MiFilterCrashDumpPte+bd (+0x1f)

[ f6:fb ]

    fffff8066300eb7d-fffff8066300eb7e  2 bytes - nt!MiFilterCrashDumpPte+17d (+0xc0)

[ 00 de:80 ba ]

    fffff8066300ebf9 - nt!MiFilterCrashDumpPte+1f9 (+0x7c)

[ f6:fb ]

    fffff8066300efac-fffff8066300efad  2 bytes - nt!MmTryIdentifyPage+3c (+0x3b3)

[ 00 de:80 ba ]

    fffff8066300efe1-fffff8066300efe2  2 bytes - nt!MmTryIdentifyPage+71 (+0x35)

[ 00 de:80 ba ]

    fffff8066300f34b - nt!MmRemoveSystemCacheFromDump+23 (+0x36a)

[ 8b:94 ]

    fffff8066300ffb2 - nt!MmAddRangeToCrashDump+32 (+0xc67)

[ 7f:88 ]

    fffff80663010bb4-fffff80663010bb5  2 bytes - nt!MiMirrorRemoveInactivePages+34 (+0xc02)

[ 00 de:80 ba ]

    fffff80663010cdb-fffff80663010cdc  2 bytes - nt!MiMirrorRemoveInactivePages+15b (+0x127)

[ 00 de:80 ba ]

    fffff80663010d5e-fffff80663010d5f  2 bytes - nt!MiMirrorRemoveInactivePages+1de (+0x83)

[ 00 de:80 ba ]

    fffff80663010f2e-fffff80663010f2f  2 bytes - nt!MiGetBaseResidentPageForBugCheck+6 (+0x1d0)

[ 00 de:80 ba ]

    fffff80663012219-fffff8066301221a  2 bytes - nt!MiBuildReservationCluster+ad (+0x12eb)

[ 00 de:80 ba ]

    fffff806630123c3-fffff806630123c4  2 bytes - nt!MiBuildReservationCluster+257 (+0x1aa)

[ 00 de:80 ba ]

    fffff806630124ad - nt!MiBuildReservationCluster+341 (+0xea)

[ f6:fb ]

    fffff80663012715-fffff80663012716  2 bytes - nt!MiBuildReservationCluster+5a9 (+0x268)

[ 00 de:80 ba ]

    fffff806630128db-fffff806630128dc  2 bytes - nt!MiGetPageForWriteCluster+47 (+0x1c6)

[ 00 de:80 ba ]

    fffff80663012f3c-fffff80663012f3d  2 bytes - nt!MiGatherPagefilePages+4bc (+0x661)

[ 00 de:80 ba ]

WARNING: !chkimg output was truncated to 50 lines. Invoke !chkimg without '-lo [num\_lines]' to view  entire output.

    fffff8066347f63e - nt!CmSaveKey+62

[ 88:91 ]

    fffff8066347f95b - nt!CmpCreateTemporaryHive+43 (+0x31d)

[ 85:8e ]

    fffff8066347fa1f - nt!CmpKeyEnumStackStartFromKcbStack+3f (+0xc4)

[ 84:8d ]

    fffff8066347fdee - nt!CmpEnumerateLayeredKey+66 (+0x3cf)

[ 80:89 ]

    fffff80663480154 - nt!CmpPromoteSingleKeyFromKcbStacks+4c (+0x366)

[ 7d:86 ]

    fffff8066348016e - nt!CmpPromoteSingleKeyFromKcbStacks+66 (+0x1a)

[ 7d:86 ]

    fffff806634802db - nt!CmpValueEnumStackStartFromKcbStack+3f (+0x16d)

[ 7b:84 ]

    fffff80663480393 - nt!CmEnumerateValueFromLayeredKey+4b (+0xb8)

[ 7b:84 ]

    fffff806634806b6 - nt!CmpGetSubKeyCountForKeyNodeStack+36 (+0x323)

[ 78:81 ]

    fffff80663480891 - nt!CmpSubtreeEnumeratorStart+6d (+0x1db)

[ 76:7f ]

    fffff80663480b9b - nt!CmpDoAccessCheckOnLayeredSubtree+4b (+0x30a)

[ 73:7c ]

    fffff80663480d9e - nt!CmpPromoteSubtree+42 (+0x203)

[ 71:7a ]

    fffff8066348146b - nt!CmpKeyEnumStackInitialize+17 (+0x6cd)

[ 6a:73 ]

    fffff806634818f0 - nt!CmpKeyEnumStackEntryInitialize+1c (+0x485)

[ 65:6e ]

    fffff80663481d43 - nt!CmpFullPromoteSingleKeyFromKeyNodeStacks+47 (+0x453)

[ 61:6a ]

    fffff80663482779 - nt!CmpValueEnumStackInitialize+19 (+0xa36)

[ 57:60 ]

    fffff806634829ef - nt!CmpSortedValueEnumStackInitialize+27 (+0x276)

[ 54:5d ]

    fffff806634843d3 - nt!PiPnpRtlServiceFilterCallback+43 (+0x19e4)

[ 3a:43 ]

    fffff80663485a78 - nt!MmStoreAllocateVirtualMemory+50 (+0x16a5)

[ 24:2d ]

    fffff80663485d53 - nt!\_PnpCreateObject+3f (+0x2db)

[ 21:2a ]

    fffff80663485e5d - nt!\_PnpCreateObjectDispatch+39 (+0x10a)

[ 20:29 ]

    fffff80663485fcb - nt!ExProcessCounterSetCallback+9b (+0x16e)

[ 1e:27 ]

    fffff80663485fdc - nt!ExProcessCounterSetCallback+ac (+0x11)

[ 1e:27 ]

    fffff80663485fee - nt!ExProcessCounterSetCallback+be (+0x12)

[ 1e:27 ]

    fffff80663486590 - nt!PpmWmiGetAllData+178 (+0x5a2)

[ 19:22 ]

    fffff80663487205 - nt!WmipQueryAllDataMultiple+7d (+0xc75)

[ 0c:15 ]

    fffff806634872d0 - nt!WmipQueryAllDataMultiple+148 (+0xcb)

[ 0b:14 ]

    fffff806634880e7-fffff806634880e8  2 bytes - nt!\_CmDeleteDevice+37 (+0xe17)

[ fd de:06 df ]

    fffff8066348845a-fffff8066348845b  2 bytes - nt!\_CmDeleteDeviceInterfaceRegKey+36 (+0x373)

[ fa de:03 df ]

    fffff80663488cef - nt!\_CmDeleteDeviceRegKey+3b (+0x895)

[ f1:fa ]

    fffff806634897ab - nt!\_CmDeleteDeviceInterface+37 (+0xabc)

[ e7:f0 ]

    fffff806634898d7 - nt!\_CmRemoveDeviceFromContainer+3b (+0x12c)

[ e5:ee ]

    fffff8066348a1e8 - nt!PiCMSetDeviceProblem+44 (+0x911)

[ dc:e5 ]

    fffff8066348aad6 - nt!PnpQueueQueryAndRemoveEvent+da (+0x8ee)

[ d3:dc ]

    fffff8066348afb4 - nt!PpDevCfgProcessDeviceReset+3c (+0x4de)

[ cf:d8 ]

    fffff8066348b62c - nt!PpDevCfgProcessDeviceClass+40 (+0x678)

[ c8:d1 ]

    fffff8066348be87 - nt!MiAllocatePerSessionProtos+d7 (+0x85b)

[ c0:c9 ]

    fffff8066348cc88 - nt!SepAdtSecurityDescriptorChangedAuditAlarm+98 (+0xe01)

[ b2:bb ]

    fffff8066348d48c - nt!AlpcpGetDataFromUserVaSafe+40 (+0x804)

[ aa:b3 ]

    fffff8066348fcf5 - nt!\_CmSetInstallerClassRegProp+41 (+0x2869)

[ 81:8a ]

    fffff80663490c83 - nt!CmFcManagerUpdateFeatureUsageSubscriptions+53 (+0xf8e)

[ 72:7b ]

    fffff806634917d4 - nt!PiIrpQueryRemoveDevice+4c (+0xb51)

[ 66:6f ]

    fffff80663491f1b - nt!MiCommitFileBackedSection+e7 (+0x747)

[ 5f:68 ]

    fffff80663492794 - nt!DbgkRegisterErrorPort+84 (+0x879)

[ 57:60 ]

    fffff80663492b8a - nt!AlpcpInitializeCompletionList+b6 (+0x3f6)

[ 53:5c ]

    fffff80663492c7f - nt!AlpcpInitializeCompletionList+1ab (+0xf5)

[ 52:5b ]

    fffff80663492e48 - nt!AlpcpInitializeCompletionList+374 (+0x1c9)

[ 50:59 ]

    fffff806634937ca - nt!KiSynchNumaCounterSetCallback+5a (+0x982)

[ 46:4f ]

    fffff806634937d8 - nt!KiSynchNumaCounterSetCallback+68 (+0x0e)

[ 46:4f ]

    fffff8066349383b - nt!KiSynchNumaCounterSetCallback+cb (+0x63)

[ 46:4f ]

WARNING: !chkimg output was truncated to 50 lines. Invoke !chkimg without '-lo [num\_lines]' to view  entire output.

    fffff806638a3cd0 - nt!HaliQuerySystemInformation+40

[ 41:4a ]

    fffff806638a607b - nt!HalpMceInitializeErrorPacketContents+13 (+0x23ab)

[ 1e:27 ]

    fffff806638a6355 - nt!KiInitializeTopologyStructures+155 (+0x2da)

[ 1b:24 ]

    fffff806638a70ff - nt!KiInitializeKernel+ef (+0xdaa)

[ 0d:16 ]

    fffff806638a7de0 - nt!PoInitializePrcb+30 (+0xce1)

[ 00:09 ]

    fffff806638a8c59 - nt!KiInitializeBootStructures+4b9 (+0xe79)

[ f2:fb ]

    fffff806638a9101 - nt!KiInitPrcb+2f5 (+0x4a8)

[ ed:f6 ]

    fffff806638a91a0 - nt!KiInitPrcb+394 (+0x9f)

[ ed:f6 ]

    fffff806638a9314 - nt!HalpMmBuildTiledMemoryMap+2c (+0x174)

[ eb:f4 ]

    fffff806638a93e9 - nt!HalpMapCR3Ex+69 (+0xd5)

[ ea:f3 ]

    fffff806638a9526 - nt!EmonCompleteInitializeProfiling+a6 (+0x13d)

[ e9:f2 ]

    fffff806638a953f - nt!EmonCompleteInitializeProfiling+bf (+0x19)

[ e9:f2 ]

    fffff806638a9bc7 - nt!KiInitializePrcbContext+6f (+0x688)

[ e2:eb ]

    fffff806638aa321 - nt!IvtInitializeIommu+261 (+0x75a)

[ db:e4 ]

    fffff806638aa4c9 - nt!IvtInitializeIommu+409 (+0x1a8)

[ d9:e2 ]

    fffff806638aa6a0 - nt!IvtInitializeIommu+5e0 (+0x1d7)

[ d8:e1 ]

    fffff806638aa7aa - nt!IvtInitializeIommu+6ea (+0x10a)

[ d7:e0 ]

    fffff806638ab5a1 - nt!KiInitializeXSaveConfiguration+51 (+0xdf7)

[ c9:d2 ]

    fffff806638abbe4 - nt!HalpMcaInitializePcrContext+ec (+0x643)

[ c2:cb ]

    fffff806638ac566 - nt!HalpPiix4Detect+82 (+0x982)

[ b9:c2 ]

    fffff806638ae3da - nt!KeInitThread+ba86 (+0x1e74)

[ 9a:a3 ]

    fffff806638afa2a - nt!EmonCompleteInitializeProfiling+65aa (+0x1650)

[ 84:8d ]

    fffff806638b0d15 - nt!HalpMcaResumeProcessorConfig+35 (+0x12eb)

[ 71:7a ]

    fffff806638b0d52 - nt!HalpMcaResumeProcessorConfig+72 (+0x3d)

[ 71:7a ]

    fffff806638b1b13 - nt!HalpBuildResumeStructures+37 (+0xdc1)

[ 63:6c ]

    fffff806638b29d4 - nt!HalpCheckLowMemoryPreSleep+ac (+0xec1)

[ 54:5d ]

    fffff806638b3ecc - nt!HalpStopLegacyUsbInterruptsInternal+30 (+0x14f8)

[ 3f:48 ]

    fffff806638b3fb1 - nt!HalpBlkInitializeIdt+21 (+0xe5)

[ 3f:48 ]

    fffff806638b409e - nt!HalpBlkInitializeProcessorState+32 (+0xed)

[ 3e:47 ]

    fffff806638b40ae - nt!HalpBlkInitializeProcessorState+42 (+0x10)

[ 3e:47 ]

    fffff806638b428c - nt!HalpBlkStartBlockedProcessor+20 (+0x1de)

[ 3c:45 ]

    fffff806638b45dc - nt!Amd64InitializeProfiling+24c (+0x350)

[ 38:41 ]

    fffff806638b462d - nt!Amd64InitializeProfiling+29d (+0x51)

[ 38:41 ]

    fffff806638b4acd - nt!IvtProcessDeviceExceptions+29 (+0x4a0)

[ 33:3c ]

    fffff806638b4b40 - nt!IvtProcessDeviceExceptions+9c (+0x73)

[ 33:3c ]

    fffff806638b4d97 - nt!HsaInitializeInterruptRemapping+bf (+0x257)

[ 31:3a ]

    fffff806638b4f73 - nt!HsaInitializeIommu+103 (+0x1dc)

[ 2f:38 ]

    fffff806638b5041 - nt!HsaInitializeIommu+1d1 (+0xce)

[ 2e:37 ]

    fffff806638b55ba - nt!HalpIvtpInitializeReservedDomain+72 (+0x579)

[ 29:32 ]

    fffff806638b65d5 - nt!PnprQuiesceDevices+31 (+0x101b)

[ 18:21 ]

    fffff806638b6be9 - nt!PnprQuiesceProcessors+45 (+0x614)

[ 12:1b ]

    fffff806638b70ff - nt!PnprQuiesceWorker+2f (+0x516)

[ 0d:16 ]

    fffff806638b73d4 - nt!IoBuildPoDeviceNotifyList+74 (+0x2d5)

[ 0a:13 ]

    fffff806638b8772-fffff806638b8773  2 bytes - nt!KiUpdateSavedSupervisorState+d6 (+0x139e)

[ f7 9b:00 9c ]

    fffff806638b889a - nt!KiInitializeDynamicProcessorDpc+3a (+0x128)

[ f6:ff ]

    fffff806638b88ff - nt!KiInitializeDynamicProcessorDpc+9f (+0x65)

[ f5:fe ]

    fffff806638bb06e - nt!PopBuildMemoryImageHeader+5a (+0x276f)

[ ce:d7 ]

    fffff806638bb42d - nt!PopCompressHiberBlocks+39 (+0x3bf)

[ ca:d3 ]

    fffff806638bb82c - nt!PopDecompressHiberBlocks+58 (+0x3ff)

[ c6:cf ]

    fffff806638bbe58 - nt!PopEndMirroring+158 (+0x62c)

[ c0:c9 ]

WARNING: !chkimg output was truncated to 50 lines. Invoke !chkimg without '-lo [num\_lines]' to view  entire output.

    fffff806638c9363 - nt!KdpReportLoadSymbolsStateChange+53

[ eb:f4 ]

    fffff806638c9ed8 - nt!KdpCreateRemoteFile+44 (+0xb75)

[ df:e8 ]

    fffff806638ca43e - nt!KdLogDbgPrint+16e (+0x566)

[ da:e3 ]

    fffff806638ca496 - nt!KdLogDbgPrint+1c6 (+0x58)

[ da:e3 ]

    fffff806638ca5be - nt!HalpRegisterDeviceInUse+7e (+0x128)

[ d8:e1 ]

    fffff806638ca739 - nt!KdSendTraceData+51 (+0x17b)

[ d7:e0 ]

    fffff806638ca9ee - nt!KdpInitializeExtendedContext+92 (+0x2b5)

[ d4:dd ]

    fffff806638cb8b9 - nt!KdpReportExceptionStateChange+51 (+0xecb)

[ c6:cf ]

    fffff806638cca6a - nt!HalpKdEnumerateDebuggingDevices+145a (+0x11b1)

[ b4:bd ]

    fffff806638ccdd4 - nt!KdpCloseRemoteFile+3c (+0x36a)

[ b0:b9 ]

    fffff806638cd043 - nt!KdpReadRemoteFile+43 (+0x26f)

[ ae:b7 ]

    fffff806638cd690 - nt!KdpReportCommandStringStateChange+50 (+0x64d)

[ a8:b1 ]

    fffff806638cd6ce - nt!KdpReportCommandStringStateChange+8e (+0x3e)

[ a7:b0 ]

    fffff80663904e1e - nt!AnFwDisplayFade+3ea

[ 30:39 ]

    fffff80663904e61 - nt!AnFwDisplayFade+42d (+0x43)

[ 30:39 ]

    fffff80663904fe2 - nt!AnFwDisplayFade+5ae (+0x181)

[ 2e:37 ]

    fffff80663906087 - nt!BgpFwLibraryInitialize+40f (+0x10a5)

[ 1e:27 ]

    fffff80663906355 - nt!BgpTxtCreateRegion+a9 (+0x2ce)

[ 1b:24 ]

    fffff8066390679e - nt!BgpConsoleInitialize+be (+0x449)

[ 17:20 ]

    fffff8066390ab10 - nt!LogFwInitialize+cc (+0x4372)

[ d3:dc ]

    fffff80663913011-fffff80663913013  3 bytes - nt!RtlFunctionOverrideSelfTest$thunk$6746816294339431247+1

[ 33 86 b6:cb db 8f ]

    fffff80663913022 - nt!memset$thunk$772440563353939046+2 (+0x11)

[ 4e:57 ]

8619 errors : !nt (fffff80662f506c0-fffff80663913022)

MODULE\_NAME: memory\_corruption

IMAGE\_NAME:  memory\_corruption

MEMORY\_CORRUPTOR:  LARGE

STACK\_COMMAND:  .cxr; .ecxr ; kb

FAILURE\_BUCKET\_ID:  LKD\_MEMORY\_CORRUPTION\_LARGE

OS\_VERSION:  10.0.25972.1000

BUILDLAB\_STR:  rs\_prerelease

OSPLATFORM\_TYPE:  x64

OSNAME:  Windows 10

FAILURE\_ID\_HASH:  {06247c58-1f9d-5de1-61a8-49cc4ccb24d5}

Followup:     memory\_corruption

---------

<https://hsdes.intel.com/appstore/article/#/22018972920>

[MTL-P] [RVP] DRIVER\_CAUGHT\_MODIFYING\_FREED\_POOL (c6) TeeDriverW10x64.sys:

0: kd> !analyze -v

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

\*                                                                             \*

\*                        Bugcheck Analysis                                    \*

\*                                                                             \*

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

DRIVER\_CAUGHT\_MODIFYING\_FREED\_POOL (c6)

An attempt was made to access freed pool memory.  The faulty component is

displayed in the current kernel stack.

Arguments:

Arg1: ffffae08eef46190, memory referenced

Arg2: 0000000000000001, value 0 = read operation, 1 = write operation

Arg3: 0000000000000000, previous mode.

Arg4: 0000000000000000, 4.

Debugging Details:

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

Unable to load image \SystemRoot\System32\DriverStore\FileRepository\heci.inf\_amd64\_96cd661731a25dc4\x64\TeeDriverW10x64.sys, Win32 error 0n2

KEY\_VALUES\_STRING: 1

    Key  : Analysis.CPU.mSec

    Value: 2686

    Key  : Analysis.DebugAnalysisManager

    Value: Create

    Key  : Analysis.Elapsed.mSec

    Value: 5466

    Key  : Analysis.Init.CPU.mSec

    Value: 3968

    Key  : Analysis.Init.Elapsed.mSec

    Value: 41835

    Key  : Analysis.Memory.CommitPeak.Mb

    Value: 99

    Key  : WER.OS.Branch

    Value: rs\_prerelease

    Key  : WER.OS.Timestamp

    Value: 2023-10-13T15:34:00Z

    Key  : WER.OS.Version

    Value: 10.0.25977.1000

FILE\_IN\_CAB:  MEMORY\_G06-MTLH-B04\_2023-10-15\_18-07-19.DMP

TAG\_NOT\_DEFINED\_202b:  \*\*\* Unknown TAG in analysis list 202b

DUMP\_FILE\_ATTRIBUTES: 0x1800

BUGCHECK\_CODE:  c6

BUGCHECK\_P1: ffffae08eef46190

BUGCHECK\_P2: 1

BUGCHECK\_P3: 0

BUGCHECK\_P4: 0

WRITE\_ADDRESS: Unable to get offset of nt!\_MI\_VISIBLE\_STATE.SessionWsList

Unable to get nt!MiVisibleState->SessionIdBitmap

MAX\_SYSTEM\_VA\_ASSIGNMENTS needs to be increased

 ffffae08eef46190 Nonpaged pool

PREVIOUS\_MODE:  0

BLACKBOXBSD: 1 (!blackboxbsd)

BLACKBOXNTFS: 1 (!blackboxntfs)

BLACKBOXPNP: 1 (!blackboxpnp)

BLACKBOXWINLOGON: 1

PROCESS\_NAME:  System

DPC\_STACK\_BASE:  FFFFF8063EB31FB0

STACK\_TEXT:

fffff806`3eb314f8 fffff806`3a6bb04c     : 00000000`000000c6 ffffae08`eef46190 00000000`00000001 00000000`00000000 : nt!KeBugCheckEx

fffff806`3eb31500 fffff806`3a4cbdf5     : fffff806`708870ac fffff806`3eb315b8 ffffae09`0fb6b000 00000000`00000017 : nt!ExpCheckForFreedEnhancedTimer+0x1ef238

fffff806`3eb31540 fffff806`3cb40bb6     : ffffae09`159f8590 fffff806`58b0509e 00000000`00000009 00000000`00000000 : nt!ExCancelTimer+0x15

fffff806`3eb31570 fffff806`58b06ddd     : 000051f6`ea607a68 fffff806`58b10000 ffffae09`15ad1e00 ffffae09`159f8590 : Wdf01000!imp\_WdfTimerStop+0xb6 [minkernel\wdf\framework\shared\core\fxtimerapi.cpp @ 293]

fffff806`3eb31600 fffff806`58b05893     : ffffae09`0faa4310 fffff806`3eb317b0 ffffae09`15ad1e70 00000000`00000000 : TeeDriverW10x64+0x36ddd

fffff806`3eb31640 fffff806`58adc5f9     : 00000000`00000127 fffff806`3eb31748 00000000`00000000 fffff806`58b100a8 : TeeDriverW10x64+0x35893

fffff806`3eb316b0 fffff806`58ad4440     : 00000000`00000000 ffffae09`0faa4310 fffff806`3eb318e8 ffffae09`0faa4310 : TeeDriverW10x64+0xc5f9

fffff806`3eb31800 fffff806`58aefcd4     : ffffae09`0faa4310 fffff806`3eb318e9 ffffae09`0faaed00 fffff806`3eb318c0 : TeeDriverW10x64+0x4440

fffff806`3eb31880 fffff806`58aeb82b     : ffffae09`0faa4310 ffffae09`0faa4310 ffffae09`0faaed48 000051f6`f05513a8 : TeeDriverW10x64+0x1fcd4

fffff806`3eb31950 fffff806`3cb53222     : 000051f6`f05513a8 ffffae09`0faaec5a ffffae09`0faaeda0 ffffae09`0faaecb0 : TeeDriverW10x64+0x1b82b

fffff806`3eb31990 fffff806`3a446eaf     : 00000000`00000000 00000000`00000000 ffffae09`0faaed00 fffff806`360949c0 : Wdf01000!FxInterrupt::\_InterruptDpcThunk+0xb2 [minkernel\wdf\framework\shared\irphandlers\pnp\km\interruptobjectkm.cpp @ 405]

fffff806`3eb319e0 fffff806`3a446256     : 00000000`00000000 00000000`00000000 fffff806`36091180 00004f14`0e616326 : nt!KiExecuteAllDpcs+0x55f

fffff806`3eb31d30 fffff806`3a66aef5     : 00000000`00000000 00000000`00000000 ffffc403`9c3c6ec0 00000000`00000000 : nt!KiRetireDpcList+0x366

fffff806`3eb31fb0 fffff806`3a66ae9f     : ffffc403`9c3c6f69 fffff806`3a450718 ffff8305`00000000 00000000`0000001a : nt!KxSwapStacksAndRetireDpcList+0x5

ffffc403`9c3c6ec0 fffff806`3a450718     : ffff8305`00000000 00000000`0000001a ffff8305`b104dce0 ffffae08`ea50adc0 : nt!KiPlatformSwapStacksAndCallReturn

ffffc403`9c3c6ed0 fffff806`3a66a38f     : ffffc403`9c3c7588 ffffae08`f3257000 ffffc403`9c3c7080 ffffc403`9c3c758c : nt!KiDispatchInterrupt+0xa8

ffffc403`9c3c6fd0 fffff806`3a4f1990     : ffffffff`ffffff80 fffff806`3a5cc074 00000000`01000010 00000000`00040282 : nt!KiDpcInterrupt+0x39f

ffffc403`9c3c7160 fffff806`3a5cc098     : 00000000`00000000 00000000`00002000 00000000`70506f50 00000000`00000000 : nt!KeReleaseQueuedSpinLock+0x70

ffffc403`9c3c7190 fffff806`3acb7b14     : ffffae08`f32570a0 00000000`00000000 ffff6d43`d60b1450 fffff806`3a5ccee3 : nt!IoGetLowerDeviceObjectWithTag+0x4c

ffffc403`9c3c71c0 fffff806`3acb749e     : ffffae08`f324e3c0 ffffc403`9c3c7230 ffffae09`1473faa0 fffff806`3a6e5551 : nt!IopCheckDeviceFlags+0x40

ffffc403`9c3c71f0 fffff806`3acc09ed     : 00000000`00000004 ffffae09`1473faa0 00000000`00000004 fffff806`3a47388b : nt!IoBuildPoDeviceNotifyList+0x13e

ffffc403`9c3c7250 fffff806`3abb577a     : 00000000`00000000 ffffae09`1473fa70 00000000`00000000 ffffc403`9c3c7518 : nt!PopBuildDeviceNotifyList+0xc5

ffffc403`9c3c7330 fffff806`3acc2b5c     : ffffc403`9c3c7518 ffffc403`9c3c7419 00000000`00000000 fffff806`3a676415 : nt!PoInitializeBroadcast+0xd6

ffffc403`9c3c7360 fffff806`3acbff2c     : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : nt!PopTransitionSystemPowerStateEx+0x2a4

ffffc403`9c3c7480 fffff806`3a676415     : fffff806`3ae2b924 ffff9c80`fe708180 00000043`9cfd1807 00000043`9cfd0040 : nt!NtSetSystemPowerState+0x4c

ffffc403`9c3c7650 fffff806`3a664e60     : fffff806`3abb3c0c 00000000`00000000 00000000`00000000 00000000`00000000 : nt!KiSystemServiceCopyEnd+0x25

ffffc403`9c3c77e8 fffff806`3abb3c0c     : 00000000`00000000 00000000`00000000 00000000`00000000 ffffffff`fffe7960 : nt!KiServiceLinkage

ffffc403`9c3c77f0 fffff806`3abb3e20     : 00000000`80000004 00000000`ffffff00 00000000`00000005 fffff806`80000004 : nt!PopIssueActionRequest+0x30c

ffffc403`9c3c7890 fffff806`3a5b0751     : ffffae09`17067000 00000000`00000000 00000000`ffffffff ffffae09`09a264e0 : nt!PopPolicyWorkerAction+0x80

ffffc403`9c3c7910 fffff806`3a4d7af5     : ffffae08`00000000 ffffae09`17067040 ffffc403`9c3c7a50 ffffc403`9c3c7a50 : nt!PopPolicyWorkerThread+0x91

ffffc403`9c3c7950 fffff806`3a5b02b3     : ffffae09`17067040 00000000`00000000 ffffae09`17067040 fffff806`3a4d79a0 : nt!ExpWorkerThread+0x155

ffffc403`9c3c7b30 fffff806`3a6644f4     : ffff9c80`fe357180 ffffae09`17067040 fffff806`3a5b0260 00000000`00000246 : nt!PspSystemThreadStartup+0x53

ffffc403`9c3c7b80 00000000`00000000     : ffffc403`9c3c8000 ffffc403`9c3c1000 00000000`00000000 00000000`00000000 : nt!KiStartSystemThread+0x34

SYMBOL\_NAME:  TeeDriverW10x64+36ddd

MODULE\_NAME: TeeDriverW10x64

IMAGE\_NAME:  TeeDriverW10x64.sys

STACK\_COMMAND:  .cxr; .ecxr ; kb

BUCKET\_ID\_FUNC\_OFFSET:  36ddd

FAILURE\_BUCKET\_ID:  0xC6\_TeeDriverW10x64!unknown\_function

OS\_VERSION:  10.0.25977.1000

BUILDLAB\_STR:  rs\_prerelease

OSPLATFORM\_TYPE:  x64

OSNAME:  Windows 10

FAILURE\_ID\_HASH:  {ee36cfb9-b34f-1956-2f5b-6751fb50438f}

Followup:     MachineOwner

---------

<https://hsdes.intel.com/appstore/article/#/22018962165>

[MTL-P] [RVP] PdcLockWatchdog A thread has been holding the PDC lock for too long:

0: kd> !analyze -v

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

\*                                                                             \*

\*                        Bugcheck Analysis                                    \*

\*                                                                             \*

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

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: ffffe605dc6cb080, The thread holding the PDC lock.

Arg2: 0000000000007530, Lock watchdog timeout in milliseconds.

Arg3: 0000000000000000, Reserved.

Arg4: 0000000000000000, Reserved.

Debugging Details:

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

KEY\_VALUES\_STRING: 1

    Key  : Analysis.CPU.mSec

    Value: 4952

    Key  : Analysis.DebugAnalysisManager

    Value: Create

    Key  : Analysis.Elapsed.mSec

    Value: 9916

    Key  : Analysis.Init.CPU.mSec

    Value: 2983

    Key  : Analysis.Init.Elapsed.mSec

    Value: 53536

    Key  : Analysis.Memory.CommitPeak.Mb

    Value: 99

    Key  : WER.OS.Branch

    Value: rs\_prerelease

    Key  : WER.OS.Timestamp

    Value: 2023-10-06T14:24:00Z

    Key  : WER.OS.Version

    Value: 10.0.25972.1000

FILE\_IN\_CAB:  PdcLockWatchdog-20231011-1448.dmp

DUMP\_FILE\_ATTRIBUTES: 0x810

  Live Generated Dump

BUGCHECK\_CODE:  17c

BUGCHECK\_P1: ffffe605dc6cb080

BUGCHECK\_P2: 7530

BUGCHECK\_P3: 0

BUGCHECK\_P4: 0

PROCESS\_NAME:  System

STACK\_TEXT:

ffffba89`893af2a0 fffff806`1ec0cee2     : 00000000`00000000 ffffba89`893af370 ffffe605`ac940040 00000000`00000000 : nt!IopLiveDumpCollectPages+0x90

ffffba89`893af2f0 fffff806`1f4a2696     : 00000000`00000000 ffffe605`ac940040 ffffba89`893af370 ffffe605`ac940040 : nt!IopLiveDumpEndMirroringCallback+0x52

ffffba89`893af320 fffff806`1ec102e1     : 00000000`00000000 fffff806`1ec0e200 ffffe605`d5151010 ffffba89`893af510 : nt!MmDuplicateMemory+0x2de

ffffba89`893af3b0 fffff806`1ec0d510     : 00000000`00000000 fffff806`1ee64d80 ffffe605`cf585dc0 00000000`00000000 : nt!IopLiveDumpCapture+0x69

ffffba89`893af410 fffff806`1ec0e626     : ffffe605`d5151010 ffffe605`d5151010 ffffbf8e`10bbd6a8 00000000`00000000 : nt!IopLiveDumpCaptureMemoryPages+0x50

ffffba89`893af550 fffff806`1f374aa4     : 00000000`00000000 ffffe605`dd5860e0 00000000`00000038 ffffbf8e`12807e60 : nt!IoCaptureLiveDump+0x30a

ffffba89`893af780 fffff806`1f375028     : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : nt!DbgkpWerCaptureLiveFullDump+0x180

ffffba89`893af7e0 fffff806`1f36c298     : ffffaa80`52590100 00000000`00000000 fffff806`226aede0 fffff806`226bd0d0 : nt!DbgkpWerProcessPolicyResult+0x30

ffffba89`893af810 fffff806`1f2b4c69     : fffff806`226bd0d0 ffffba89`893afa50 ffffe605`ac6e8540 fffff806`226aebdb : nt!DbgkWerCaptureLiveKernelDump2+0xb7618

ffffba89`893af870 fffff806`226aee64     : fffff806`226bd0d0 ffffe605`00000000 00000000`00000000 fffff806`1edb06b3 : nt!DbgkWerCaptureLiveKernelDump+0x69

ffffba89`893af8f0 fffff806`1ecd7aa5     : ffffe605`ac6e8540 ffffe605`ac940040 ffffba89`893afa00 ffffba89`893afa50 : pdc!PdcpLockWatchdogWorkerRoutine+0x84

ffffba89`893af950 fffff806`1edb01d3     : ffffe605`ac940040 00000000`00000000 ffffe605`ac940040 fffff806`1ecd7950 : nt!ExpWorkerThread+0x155

ffffba89`893afb30 fffff806`1ee64414     : ffffaa80`52590180 ffffe605`ac940040 fffff806`1edb0180 00000000`00000000 : nt!PspSystemThreadStartup+0x53

ffffba89`893afb80 00000000`00000000     : ffffba89`893b0000 ffffba89`893a9000 00000000`00000000 00000000`00000000 : nt!KiStartSystemThread+0x34

CHKIMG\_EXTENSION: !chkimg -lo 50 -d !nt

    fffff8061eb506c0-fffff8061eb506c2  3 bytes - nt!\_guard\_check\_icall\_fptr

[ 20 4f d3:c0 bf e6 ]

    fffff8061eb506c8-fffff8061eb506ca  3 bytes - nt!\_guard\_dispatch\_icall\_fptr (+0x08)

[ 70 e2 e5:10 c0 e6 ]

    fffff8061ec00165 - nt!RtlCompressBufferXpressHuffStandard+e5

[ 7d:86 ]

    fffff8061ec008b6 - nt!XpressBuildHuffmanEncodings+26 (+0x751)

[ 76:7f ]

    fffff8061ec008ca - nt!XpressBuildHuffmanEncodings+3a (+0x14)

[ 75:7e ]

    fffff8061ec008e8 - nt!XpressBuildHuffmanEncodings+58 (+0x1e)

[ 75:7e ]

    fffff8061ec0094d - nt!XpressBuildHuffmanEncodings+bd (+0x65)

[ 75:7e ]

    fffff8061ec00fec - nt!LZ4\_compress\_fast\_extState+4c (+0x69f)

[ 6e:77 ]

    fffff8061ec0143f - nt!LZ4\_compress\_fast\_extState+49f (+0x453)

[ 6a:73 ]

    fffff8061ec01474 - nt!LZ4\_compress\_fast\_extState+4d4 (+0x35)

[ 6a:73 ]

    fffff8061ec01e50 - nt!B\_TREE<\_SM\_PAGE\_KEY,SMKM\_STORE\_MGR<SM\_TRAITS>::SMKM\_FRONTEND\_ENTRY,4096,B\_TREE\_DUMMY\_NODE\_POOL,B\_TREE\_KEY\_COMPARATOR<\_SM\_PAGE\_KEY> >::BTreeNewNode+3c (+0x9dc)

[ 60:69 ]

    fffff8061ec01eba - nt!ST\_STORE<SM\_TRAITS>::StCompactionPickPriority+42 (+0x6a)

[ 60:69 ]

    fffff8061ec024f5 - nt!ST\_STORE<SM\_TRAITS>::StCompactionPerformInMem+49 (+0x63b)

[ 59:62 ]

    fffff8061ec03b02 - nt!SMKM\_STORE\_MGR<SM\_TRAITS>::SmFeAddComplete+46 (+0x160d)

[ 43:4c ]

    fffff8061ec03ef8 - nt!SMKM\_STORE\_MGR<SM\_TRAITS>::SmFeEvictComplete+48 (+0x3f6)

[ 3f:48 ]

    fffff8061ec04e54 - nt!ST\_STORE<SM\_TRAITS>::StCompactRegions+54 (+0xf5c)

[ 30:39 ]

    fffff8061ec0a039 - nt!SmBinaryArrayGrow+89 (+0x51e5)

[ de:e7 ]

    fffff8061ec0a2d6 - nt!B\_TREE<unsigned long,ST\_STORE<SM\_TRAITS>::\_ST\_HASH\_ENTRY,4096,NP\_CONTEXT,ST\_STORE<SM\_TRAITS>::ST\_HASH\_ENTRY\_COMPARATOR>::BTreeNewNode+3e (+0x29d)

[ db:e4 ]

    fffff8061ec0ad57 - nt!SmArrayGrow+7b (+0xa81)

[ d1:da ]

    fffff8061ec0af12 - nt!IoFillDumpHeader+11e (+0x1bb)

[ cf:d8 ]

    fffff8061ec0af26 - nt!IoFillDumpHeader+132 (+0x14)

[ cf:d8 ]

    fffff8061ec0c41b - nt!MiMapMemoryDumpMdl+43 (+0x14f5)

[ ba:c3 ]

    fffff8061ec0c455-fffff8061ec0c456  2 bytes - nt!MiMapMemoryDumpMdl+7d (+0x3a)

[ 80 f6:00 89 ]

    fffff8061ec0c541-fffff8061ec0c542  2 bytes - nt!MiMapMemoryDumpMdl+169 (+0xec)

[ 80 f6:00 89 ]

    fffff8061ec0c569-fffff8061ec0c56a  2 bytes - nt!MiMapMemoryDumpMdl+191 (+0x28)

[ 00 de:80 8a ]

    fffff8061ec0cc74-fffff8061ec0cc75  2 bytes - nt!MmFreeIndependentPages+64 (+0x70b)

[ 80 f6:00 89 ]

    fffff8061ec0ccb6-fffff8061ec0ccb7  2 bytes - nt!MmFreeIndependentPages+a6 (+0x42)

[ 00 de:80 8a ]

    fffff8061ec0cdb6-fffff8061ec0cdb7  2 bytes - nt!MmFreeIndependentPages+1a6 (+0x100)

[ 00 de:80 8a ]

    fffff8061ec0d02e - nt!IopLiveDumpCollectPages+b6 (+0x278)

[ ae:b7 ]

    fffff8061ec0d30e - nt!IopLiveDumpEstimateMemoryPages+fa (+0x2e0)

[ ab:b4 ]

    fffff8061ec0d337 - nt!IopLiveDumpEstimateMemoryPages+123 (+0x29)

[ ab:b4 ]

    fffff8061ec0d360 - nt!IopLiveDumpEstimateMemoryPages+14c (+0x29)

[ ab:b4 ]

    fffff8061ec0d970 - nt!IopLiveDumpAllocAndInitResources+1e4 (+0x610)

[ a5:ae ]

    fffff8061ec0ea81-fffff8061ec0ea82  2 bytes - nt!MiFilterCrashDumpPte+81 (+0x1111)

[ 00 de:80 8a ]

    fffff8061ec0ea9e-fffff8061ec0ea9f  2 bytes - nt!MiFilterCrashDumpPte+9e (+0x1d)

[ 00 de:80 8a ]

    fffff8061ec0eabc-fffff8061ec0eabd  2 bytes - nt!MiFilterCrashDumpPte+bc (+0x1e)

[ 80 f6:00 89 ]

    fffff8061ec0eb7d-fffff8061ec0eb7e  2 bytes - nt!MiFilterCrashDumpPte+17d (+0xc1)

[ 00 de:80 8a ]

    fffff8061ec0ebf8-fffff8061ec0ebf9  2 bytes - nt!MiFilterCrashDumpPte+1f8 (+0x7b)

[ 80 f6:00 89 ]

    fffff8061ec0efac-fffff8061ec0efad  2 bytes - nt!MmTryIdentifyPage+3c (+0x3b4)

[ 00 de:80 8a ]

    fffff8061ec0efe1-fffff8061ec0efe2  2 bytes - nt!MmTryIdentifyPage+71 (+0x35)

[ 00 de:80 8a ]

    fffff8061ec0f34b - nt!MmRemoveSystemCacheFromDump+23 (+0x36a)

[ 8b:94 ]

    fffff8061ec0ffb2 - nt!MmAddRangeToCrashDump+32 (+0xc67)

[ 7f:88 ]

    fffff8061ec10bb4-fffff8061ec10bb5  2 bytes - nt!MiMirrorRemoveInactivePages+34 (+0xc02)

[ 00 de:80 8a ]

    fffff8061ec10cdb-fffff8061ec10cdc  2 bytes - nt!MiMirrorRemoveInactivePages+15b (+0x127)

[ 00 de:80 8a ]

    fffff8061ec10d5e-fffff8061ec10d5f  2 bytes - nt!MiMirrorRemoveInactivePages+1de (+0x83)

[ 00 de:80 8a ]

    fffff8061ec10f2e-fffff8061ec10f2f  2 bytes - nt!MiGetBaseResidentPageForBugCheck+6 (+0x1d0)

[ 00 de:80 8a ]

    fffff8061ec12219-fffff8061ec1221a  2 bytes - nt!MiBuildReservationCluster+ad (+0x12eb)

[ 00 de:80 8a ]

    fffff8061ec123c3-fffff8061ec123c4  2 bytes - nt!MiBuildReservationCluster+257 (+0x1aa)

[ 00 de:80 8a ]

    fffff8061ec124ac-fffff8061ec124ad  2 bytes - nt!MiBuildReservationCluster+340 (+0xe9)

[ 80 f6:00 89 ]

    fffff8061ec12715-fffff8061ec12716  2 bytes - nt!MiBuildReservationCluster+5a9 (+0x269)

[ 00 de:80 8a ]

    fffff8061ec128db-fffff8061ec128dc  2 bytes - nt!MiGetPageForWriteCluster+47 (+0x1c6)

[ 00 de:80 8a ]

    fffff8061ec12f3c-fffff8061ec12f3d  2 bytes - nt!MiGatherPagefilePages+4bc (+0x661)

[ 00 de:80 8a ]

WARNING: !chkimg output was truncated to 50 lines. Invoke !chkimg without '-lo [num\_lines]' to view  entire output.

    fffff8061f07f63e - nt!CmSaveKey+62

[ 88:91 ]

    fffff8061f07f95b - nt!CmpCreateTemporaryHive+43 (+0x31d)

[ 85:8e ]

    fffff8061f07fa1f - nt!CmpKeyEnumStackStartFromKcbStack+3f (+0xc4)

[ 84:8d ]

    fffff8061f07fdee - nt!CmpEnumerateLayeredKey+66 (+0x3cf)

[ 80:89 ]

    fffff8061f080154 - nt!CmpPromoteSingleKeyFromKcbStacks+4c (+0x366)

[ 7d:86 ]

    fffff8061f08016e - nt!CmpPromoteSingleKeyFromKcbStacks+66 (+0x1a)

[ 7d:86 ]

    fffff8061f0802db - nt!CmpValueEnumStackStartFromKcbStack+3f (+0x16d)

[ 7b:84 ]

    fffff8061f080393 - nt!CmEnumerateValueFromLayeredKey+4b (+0xb8)

[ 7b:84 ]

    fffff8061f0806b6 - nt!CmpGetSubKeyCountForKeyNodeStack+36 (+0x323)

[ 78:81 ]

    fffff8061f080891 - nt!CmpSubtreeEnumeratorStart+6d (+0x1db)

[ 76:7f ]

    fffff8061f080b9b - nt!CmpDoAccessCheckOnLayeredSubtree+4b (+0x30a)

[ 73:7c ]

    fffff8061f080d9e - nt!CmpPromoteSubtree+42 (+0x203)

[ 71:7a ]

    fffff8061f08146b - nt!CmpKeyEnumStackInitialize+17 (+0x6cd)

[ 6a:73 ]

    fffff8061f0818f0 - nt!CmpKeyEnumStackEntryInitialize+1c (+0x485)

[ 65:6e ]

    fffff8061f081d43 - nt!CmpFullPromoteSingleKeyFromKeyNodeStacks+47 (+0x453)

[ 61:6a ]

    fffff8061f082779 - nt!CmpValueEnumStackInitialize+19 (+0xa36)

[ 57:60 ]

    fffff8061f0829ef - nt!CmpSortedValueEnumStackInitialize+27 (+0x276)

[ 54:5d ]

    fffff8061f0843d3 - nt!PiPnpRtlServiceFilterCallback+43 (+0x19e4)

[ 3a:43 ]

    fffff8061f085a78 - nt!MmStoreAllocateVirtualMemory+50 (+0x16a5)

[ 24:2d ]

    fffff8061f085d53 - nt!\_PnpCreateObject+3f (+0x2db)

[ 21:2a ]

    fffff8061f085e5d - nt!\_PnpCreateObjectDispatch+39 (+0x10a)

[ 20:29 ]

    fffff8061f085fcb - nt!ExProcessCounterSetCallback+9b (+0x16e)

[ 1e:27 ]

    fffff8061f085fdc - nt!ExProcessCounterSetCallback+ac (+0x11)

[ 1e:27 ]

    fffff8061f085fee - nt!ExProcessCounterSetCallback+be (+0x12)

[ 1e:27 ]

    fffff8061f086590 - nt!PpmWmiGetAllData+178 (+0x5a2)

[ 19:22 ]

    fffff8061f087205 - nt!WmipQueryAllDataMultiple+7d (+0xc75)

[ 0c:15 ]

    fffff8061f0872d0 - nt!WmipQueryAllDataMultiple+148 (+0xcb)

[ 0b:14 ]

    fffff8061f0880e7-fffff8061f0880e8  2 bytes - nt!\_CmDeleteDevice+37 (+0xe17)

[ fd de:06 df ]

    fffff8061f08845a-fffff8061f08845b  2 bytes - nt!\_CmDeleteDeviceInterfaceRegKey+36 (+0x373)

[ fa de:03 df ]

    fffff8061f088cef - nt!\_CmDeleteDeviceRegKey+3b (+0x895)

[ f1:fa ]

    fffff8061f0897ab - nt!\_CmDeleteDeviceInterface+37 (+0xabc)

[ e7:f0 ]

    fffff8061f0898d7 - nt!\_CmRemoveDeviceFromContainer+3b (+0x12c)

[ e5:ee ]

    fffff8061f08a1e8 - nt!PiCMSetDeviceProblem+44 (+0x911)

[ dc:e5 ]

    fffff8061f08aad6 - nt!PnpQueueQueryAndRemoveEvent+da (+0x8ee)

[ d3:dc ]

    fffff8061f08afb4 - nt!PpDevCfgProcessDeviceReset+3c (+0x4de)

[ cf:d8 ]

    fffff8061f08b62c - nt!PpDevCfgProcessDeviceClass+40 (+0x678)

[ c8:d1 ]

    fffff8061f08be87 - nt!MiAllocatePerSessionProtos+d7 (+0x85b)

[ c0:c9 ]

    fffff8061f08cc88 - nt!SepAdtSecurityDescriptorChangedAuditAlarm+98 (+0xe01)

[ b2:bb ]

    fffff8061f08d48c - nt!AlpcpGetDataFromUserVaSafe+40 (+0x804)

[ aa:b3 ]

    fffff8061f08fcf5 - nt!\_CmSetInstallerClassRegProp+41 (+0x2869)

[ 81:8a ]

    fffff8061f090c83 - nt!CmFcManagerUpdateFeatureUsageSubscriptions+53 (+0xf8e)

[ 72:7b ]

    fffff8061f0917d4 - nt!PiIrpQueryRemoveDevice+4c (+0xb51)

[ 66:6f ]

    fffff8061f091f1b - nt!MiCommitFileBackedSection+e7 (+0x747)

[ 5f:68 ]

    fffff8061f092794 - nt!DbgkRegisterErrorPort+84 (+0x879)

[ 57:60 ]

    fffff8061f092b8a - nt!AlpcpInitializeCompletionList+b6 (+0x3f6)

[ 53:5c ]

    fffff8061f092c7f - nt!AlpcpInitializeCompletionList+1ab (+0xf5)

[ 52:5b ]

    fffff8061f092e48 - nt!AlpcpInitializeCompletionList+374 (+0x1c9)

[ 50:59 ]

    fffff8061f0937ca - nt!KiSynchNumaCounterSetCallback+5a (+0x982)

[ 46:4f ]

    fffff8061f0937d8 - nt!KiSynchNumaCounterSetCallback+68 (+0x0e)

[ 46:4f ]

    fffff8061f09383b - nt!KiSynchNumaCounterSetCallback+cb (+0x63)

[ 46:4f ]

WARNING: !chkimg output was truncated to 50 lines. Invoke !chkimg without '-lo [num\_lines]' to view  entire output.

    fffff8061f4a3cd0 - nt!HaliQuerySystemInformation+40

[ 41:4a ]

    fffff8061f4a607b - nt!HalpMceInitializeErrorPacketContents+13 (+0x23ab)

[ 1e:27 ]

    fffff8061f4a6355 - nt!KiInitializeTopologyStructures+155 (+0x2da)

[ 1b:24 ]

    fffff8061f4a70ff - nt!KiInitializeKernel+ef (+0xdaa)

[ 0d:16 ]

    fffff8061f4a7de0 - nt!PoInitializePrcb+30 (+0xce1)

[ 00:09 ]

    fffff8061f4a8c59 - nt!KiInitializeBootStructures+4b9 (+0xe79)

[ f2:fb ]

    fffff8061f4a9101 - nt!KiInitPrcb+2f5 (+0x4a8)

[ ed:f6 ]

    fffff8061f4a91a0 - nt!KiInitPrcb+394 (+0x9f)

[ ed:f6 ]

    fffff8061f4a9314 - nt!HalpMmBuildTiledMemoryMap+2c (+0x174)

[ eb:f4 ]

    fffff8061f4a93e9 - nt!HalpMapCR3Ex+69 (+0xd5)

[ ea:f3 ]

    fffff8061f4a9526 - nt!EmonCompleteInitializeProfiling+a6 (+0x13d)

[ e9:f2 ]

    fffff8061f4a953f - nt!EmonCompleteInitializeProfiling+bf (+0x19)

[ e9:f2 ]

    fffff8061f4a9bc7 - nt!KiInitializePrcbContext+6f (+0x688)

[ e2:eb ]

    fffff8061f4aa321 - nt!IvtInitializeIommu+261 (+0x75a)

[ db:e4 ]

    fffff8061f4aa4c9 - nt!IvtInitializeIommu+409 (+0x1a8)

[ d9:e2 ]

    fffff8061f4aa6a0 - nt!IvtInitializeIommu+5e0 (+0x1d7)

[ d8:e1 ]

    fffff8061f4aa7aa - nt!IvtInitializeIommu+6ea (+0x10a)

[ d7:e0 ]

    fffff8061f4ab5a1 - nt!KiInitializeXSaveConfiguration+51 (+0xdf7)

[ c9:d2 ]

    fffff8061f4abbe4 - nt!HalpMcaInitializePcrContext+ec (+0x643)

[ c2:cb ]

    fffff8061f4ac566 - nt!HalpPiix4Detect+82 (+0x982)

[ b9:c2 ]

    fffff8061f4ae3da - nt!KeInitThread+ba86 (+0x1e74)

[ 9a:a3 ]

    fffff8061f4afa2a - nt!EmonCompleteInitializeProfiling+65aa (+0x1650)

[ 84:8d ]

    fffff8061f4b0d15 - nt!HalpMcaResumeProcessorConfig+35 (+0x12eb)

[ 71:7a ]

    fffff8061f4b0d52 - nt!HalpMcaResumeProcessorConfig+72 (+0x3d)

[ 71:7a ]

    fffff8061f4b1b13 - nt!HalpBuildResumeStructures+37 (+0xdc1)

[ 63:6c ]

    fffff8061f4b29d4 - nt!HalpCheckLowMemoryPreSleep+ac (+0xec1)

[ 54:5d ]

    fffff8061f4b3ecc - nt!HalpStopLegacyUsbInterruptsInternal+30 (+0x14f8)

[ 3f:48 ]

    fffff8061f4b3fb1 - nt!HalpBlkInitializeIdt+21 (+0xe5)

[ 3f:48 ]

    fffff8061f4b409e - nt!HalpBlkInitializeProcessorState+32 (+0xed)

[ 3e:47 ]

    fffff8061f4b40ae - nt!HalpBlkInitializeProcessorState+42 (+0x10)

[ 3e:47 ]

    fffff8061f4b428c - nt!HalpBlkStartBlockedProcessor+20 (+0x1de)

[ 3c:45 ]

    fffff8061f4b45dc - nt!Amd64InitializeProfiling+24c (+0x350)

[ 38:41 ]

    fffff8061f4b462d - nt!Amd64InitializeProfiling+29d (+0x51)

[ 38:41 ]

    fffff8061f4b4acd - nt!IvtProcessDeviceExceptions+29 (+0x4a0)

[ 33:3c ]

    fffff8061f4b4b40 - nt!IvtProcessDeviceExceptions+9c (+0x73)

[ 33:3c ]

    fffff8061f4b4d97 - nt!HsaInitializeInterruptRemapping+bf (+0x257)

[ 31:3a ]

    fffff8061f4b4f73 - nt!HsaInitializeIommu+103 (+0x1dc)

[ 2f:38 ]

    fffff8061f4b5041 - nt!HsaInitializeIommu+1d1 (+0xce)

[ 2e:37 ]

    fffff8061f4b55ba - nt!HalpIvtpInitializeReservedDomain+72 (+0x579)

[ 29:32 ]

    fffff8061f4b65d5 - nt!PnprQuiesceDevices+31 (+0x101b)

[ 18:21 ]

    fffff8061f4b6be9 - nt!PnprQuiesceProcessors+45 (+0x614)

[ 12:1b ]

    fffff8061f4b70ff - nt!PnprQuiesceWorker+2f (+0x516)

[ 0d:16 ]

    fffff8061f4b73d4 - nt!IoBuildPoDeviceNotifyList+74 (+0x2d5)

[ 0a:13 ]

    fffff8061f4b8772-fffff8061f4b8773  2 bytes - nt!KiUpdateSavedSupervisorState+d6 (+0x139e)

[ f7 9b:00 9c ]

    fffff8061f4b889a - nt!KiInitializeDynamicProcessorDpc+3a (+0x128)

[ f6:ff ]

    fffff8061f4b88ff - nt!KiInitializeDynamicProcessorDpc+9f (+0x65)

[ f5:fe ]

    fffff8061f4bb06e - nt!PopBuildMemoryImageHeader+5a (+0x276f)

[ ce:d7 ]

    fffff8061f4bb42d - nt!PopCompressHiberBlocks+39 (+0x3bf)

[ ca:d3 ]

    fffff8061f4bb82c - nt!PopDecompressHiberBlocks+58 (+0x3ff)

[ c6:cf ]

    fffff8061f4bbe58 - nt!PopEndMirroring+158 (+0x62c)

[ c0:c9 ]

WARNING: !chkimg output was truncated to 50 lines. Invoke !chkimg without '-lo [num\_lines]' to view  entire output.

    fffff8061f4c9363 - nt!KdpReportLoadSymbolsStateChange+53

[ eb:f4 ]

    fffff8061f4c9ed8 - nt!KdpCreateRemoteFile+44 (+0xb75)

[ df:e8 ]

    fffff8061f4ca43e - nt!KdLogDbgPrint+16e (+0x566)

[ da:e3 ]

    fffff8061f4ca496 - nt!KdLogDbgPrint+1c6 (+0x58)

[ da:e3 ]

    fffff8061f4ca5be - nt!HalpRegisterDeviceInUse+7e (+0x128)

[ d8:e1 ]

    fffff8061f4ca739 - nt!KdSendTraceData+51 (+0x17b)

[ d7:e0 ]

    fffff8061f4ca9ee - nt!KdpInitializeExtendedContext+92 (+0x2b5)

[ d4:dd ]

    fffff8061f4cb8b9 - nt!KdpReportExceptionStateChange+51 (+0xecb)

[ c6:cf ]

    fffff8061f4cca6a - nt!HalpKdEnumerateDebuggingDevices+145a (+0x11b1)

[ b4:bd ]

    fffff8061f4ccdd4 - nt!KdpCloseRemoteFile+3c (+0x36a)

[ b0:b9 ]

    fffff8061f4cd043 - nt!KdpReadRemoteFile+43 (+0x26f)

[ ae:b7 ]

    fffff8061f4cd690 - nt!KdpReportCommandStringStateChange+50 (+0x64d)

[ a8:b1 ]

    fffff8061f4cd6ce - nt!KdpReportCommandStringStateChange+8e (+0x3e)

[ a7:b0 ]

    fffff8061f504e1e - nt!AnFwDisplayFade+3ea

[ 30:39 ]

    fffff8061f504e61 - nt!AnFwDisplayFade+42d (+0x43)

[ 30:39 ]

    fffff8061f504fe2 - nt!AnFwDisplayFade+5ae (+0x181)

[ 2e:37 ]

    fffff8061f506087 - nt!BgpFwLibraryInitialize+40f (+0x10a5)

[ 1e:27 ]

    fffff8061f506355 - nt!BgpTxtCreateRegion+a9 (+0x2ce)

[ 1b:24 ]

    fffff8061f50679e - nt!BgpConsoleInitialize+be (+0x449)

[ 17:20 ]

    fffff8061f50ab10 - nt!LogFwInitialize+cc (+0x4372)

[ d3:dc ]

    fffff8061f513011-fffff8061f513013  3 bytes - nt!RtlFunctionOverrideSelfTest$thunk$6746816294339431247+1

[ 33 86 b6:cb db 8f ]

    fffff8061f513022 - nt!memset$thunk$772440563353939046+2 (+0x11)

[ 4e:57 ]

9661 errors : !nt (fffff8061eb506c0-fffff8061f513022)

MODULE\_NAME: memory\_corruption

IMAGE\_NAME:  memory\_corruption

MEMORY\_CORRUPTOR:  LARGE

STACK\_COMMAND:  .cxr; .ecxr ; kb

FAILURE\_BUCKET\_ID:  LKD\_MEMORY\_CORRUPTION\_LARGE

OS\_VERSION:  10.0.25972.1000

BUILDLAB\_STR:  rs\_prerelease

OSPLATFORM\_TYPE:  x64

OSNAME:  Windows 10

FAILURE\_ID\_HASH:  {06247c58-1f9d-5de1-61a8-49cc4ccb24d5}

Followup:     memory\_corruption

---------

0: kd> !analyze -v

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

\*                                                                             \*

\*                        Bugcheck Analysis                                    \*

\*                                                                             \*

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

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: ffffe605dc6cb080, The thread holding the PDC lock.

Arg2: 0000000000007530, Lock watchdog timeout in milliseconds.

Arg3: 0000000000000000, Reserved.

Arg4: 0000000000000000, Reserved.

Debugging Details:

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

KEY\_VALUES\_STRING: 1

    Key  : Analysis.CPU.mSec

    Value: 4952

    Key  : Analysis.DebugAnalysisManager

    Value: Create

    Key  : Analysis.Elapsed.mSec

    Value: 9916

    Key  : Analysis.Init.CPU.mSec

    Value: 2983

    Key  : Analysis.Init.Elapsed.mSec

    Value: 53536

    Key  : Analysis.Memory.CommitPeak.Mb

    Value: 99

    Key  : WER.OS.Branch

    Value: rs\_prerelease

    Key  : WER.OS.Timestamp

    Value: 2023-10-06T14:24:00Z

    Key  : WER.OS.Version

    Value: 10.0.25972.1000

FILE\_IN\_CAB:  PdcLockWatchdog-20231011-1448.dmp

DUMP\_FILE\_ATTRIBUTES: 0x810

  Live Generated Dump

BUGCHECK\_CODE:  17c

BUGCHECK\_P1: ffffe605dc6cb080

BUGCHECK\_P2: 7530

BUGCHECK\_P3: 0

BUGCHECK\_P4: 0

PROCESS\_NAME:  System

STACK\_TEXT:

ffffba89`893af2a0 fffff806`1ec0cee2     : 00000000`00000000 ffffba89`893af370 ffffe605`ac940040 00000000`00000000 : nt!IopLiveDumpCollectPages+0x90

ffffba89`893af2f0 fffff806`1f4a2696     : 00000000`00000000 ffffe605`ac940040 ffffba89`893af370 ffffe605`ac940040 : nt!IopLiveDumpEndMirroringCallback+0x52

ffffba89`893af320 fffff806`1ec102e1     : 00000000`00000000 fffff806`1ec0e200 ffffe605`d5151010 ffffba89`893af510 : nt!MmDuplicateMemory+0x2de

ffffba89`893af3b0 fffff806`1ec0d510     : 00000000`00000000 fffff806`1ee64d80 ffffe605`cf585dc0 00000000`00000000 : nt!IopLiveDumpCapture+0x69

ffffba89`893af410 fffff806`1ec0e626     : ffffe605`d5151010 ffffe605`d5151010 ffffbf8e`10bbd6a8 00000000`00000000 : nt!IopLiveDumpCaptureMemoryPages+0x50

ffffba89`893af550 fffff806`1f374aa4     : 00000000`00000000 ffffe605`dd5860e0 00000000`00000038 ffffbf8e`12807e60 : nt!IoCaptureLiveDump+0x30a

ffffba89`893af780 fffff806`1f375028     : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : nt!DbgkpWerCaptureLiveFullDump+0x180

ffffba89`893af7e0 fffff806`1f36c298     : ffffaa80`52590100 00000000`00000000 fffff806`226aede0 fffff806`226bd0d0 : nt!DbgkpWerProcessPolicyResult+0x30

ffffba89`893af810 fffff806`1f2b4c69     : fffff806`226bd0d0 ffffba89`893afa50 ffffe605`ac6e8540 fffff806`226aebdb : nt!DbgkWerCaptureLiveKernelDump2+0xb7618

ffffba89`893af870 fffff806`226aee64     : fffff806`226bd0d0 ffffe605`00000000 00000000`00000000 fffff806`1edb06b3 : nt!DbgkWerCaptureLiveKernelDump+0x69

ffffba89`893af8f0 fffff806`1ecd7aa5     : ffffe605`ac6e8540 ffffe605`ac940040 ffffba89`893afa00 ffffba89`893afa50 : pdc!PdcpLockWatchdogWorkerRoutine+0x84

ffffba89`893af950 fffff806`1edb01d3     : ffffe605`ac940040 00000000`00000000 ffffe605`ac940040 fffff806`1ecd7950 : nt!ExpWorkerThread+0x155

ffffba89`893afb30 fffff806`1ee64414     : ffffaa80`52590180 ffffe605`ac940040 fffff806`1edb0180 00000000`00000000 : nt!PspSystemThreadStartup+0x53

ffffba89`893afb80 00000000`00000000     : ffffba89`893b0000 ffffba89`893a9000 00000000`00000000 00000000`00000000 : nt!KiStartSystemThread+0x34

CHKIMG\_EXTENSION: !chkimg -lo 50 -d !nt

    fffff8061eb506c0-fffff8061eb506c2  3 bytes - nt!\_guard\_check\_icall\_fptr

[ 20 4f d3:c0 bf e6 ]

    fffff8061eb506c8-fffff8061eb506ca  3 bytes - nt!\_guard\_dispatch\_icall\_fptr (+0x08)

[ 70 e2 e5:10 c0 e6 ]

    fffff8061ec00165 - nt!RtlCompressBufferXpressHuffStandard+e5

[ 7d:86 ]

    fffff8061ec008b6 - nt!XpressBuildHuffmanEncodings+26 (+0x751)

[ 76:7f ]

    fffff8061ec008ca - nt!XpressBuildHuffmanEncodings+3a (+0x14)

[ 75:7e ]

    fffff8061ec008e8 - nt!XpressBuildHuffmanEncodings+58 (+0x1e)

[ 75:7e ]

    fffff8061ec0094d - nt!XpressBuildHuffmanEncodings+bd (+0x65)

[ 75:7e ]

    fffff8061ec00fec - nt!LZ4\_compress\_fast\_extState+4c (+0x69f)

[ 6e:77 ]

    fffff8061ec0143f - nt!LZ4\_compress\_fast\_extState+49f (+0x453)

[ 6a:73 ]

    fffff8061ec01474 - nt!LZ4\_compress\_fast\_extState+4d4 (+0x35)

[ 6a:73 ]

    fffff8061ec01e50 - nt!B\_TREE<\_SM\_PAGE\_KEY,SMKM\_STORE\_MGR<SM\_TRAITS>::SMKM\_FRONTEND\_ENTRY,4096,B\_TREE\_DUMMY\_NODE\_POOL,B\_TREE\_KEY\_COMPARATOR<\_SM\_PAGE\_KEY> >::BTreeNewNode+3c (+0x9dc)

[ 60:69 ]

    fffff8061ec01eba - nt!ST\_STORE<SM\_TRAITS>::StCompactionPickPriority+42 (+0x6a)

[ 60:69 ]

    fffff8061ec024f5 - nt!ST\_STORE<SM\_TRAITS>::StCompactionPerformInMem+49 (+0x63b)

[ 59:62 ]

    fffff8061ec03b02 - nt!SMKM\_STORE\_MGR<SM\_TRAITS>::SmFeAddComplete+46 (+0x160d)

[ 43:4c ]

    fffff8061ec03ef8 - nt!SMKM\_STORE\_MGR<SM\_TRAITS>::SmFeEvictComplete+48 (+0x3f6)

[ 3f:48 ]

    fffff8061ec04e54 - nt!ST\_STORE<SM\_TRAITS>::StCompactRegions+54 (+0xf5c)

[ 30:39 ]

    fffff8061ec0a039 - nt!SmBinaryArrayGrow+89 (+0x51e5)

[ de:e7 ]

    fffff8061ec0a2d6 - nt!B\_TREE<unsigned long,ST\_STORE<SM\_TRAITS>::\_ST\_HASH\_ENTRY,4096,NP\_CONTEXT,ST\_STORE<SM\_TRAITS>::ST\_HASH\_ENTRY\_COMPARATOR>::BTreeNewNode+3e (+0x29d)

[ db:e4 ]

    fffff8061ec0ad57 - nt!SmArrayGrow+7b (+0xa81)

[ d1:da ]

    fffff8061ec0af12 - nt!IoFillDumpHeader+11e (+0x1bb)

[ cf:d8 ]

    fffff8061ec0af26 - nt!IoFillDumpHeader+132 (+0x14)

[ cf:d8 ]

    fffff8061ec0c41b - nt!MiMapMemoryDumpMdl+43 (+0x14f5)

[ ba:c3 ]

    fffff8061ec0c455-fffff8061ec0c456  2 bytes - nt!MiMapMemoryDumpMdl+7d (+0x3a)

[ 80 f6:00 89 ]

    fffff8061ec0c541-fffff8061ec0c542  2 bytes - nt!MiMapMemoryDumpMdl+169 (+0xec)

[ 80 f6:00 89 ]

    fffff8061ec0c569-fffff8061ec0c56a  2 bytes - nt!MiMapMemoryDumpMdl+191 (+0x28)

[ 00 de:80 8a ]

    fffff8061ec0cc74-fffff8061ec0cc75  2 bytes - nt!MmFreeIndependentPages+64 (+0x70b)

[ 80 f6:00 89 ]

    fffff8061ec0ccb6-fffff8061ec0ccb7  2 bytes - nt!MmFreeIndependentPages+a6 (+0x42)

[ 00 de:80 8a ]

    fffff8061ec0cdb6-fffff8061ec0cdb7  2 bytes - nt!MmFreeIndependentPages+1a6 (+0x100)

[ 00 de:80 8a ]

    fffff8061ec0d02e - nt!IopLiveDumpCollectPages+b6 (+0x278)

[ ae:b7 ]

    fffff8061ec0d30e - nt!IopLiveDumpEstimateMemoryPages+fa (+0x2e0)

[ ab:b4 ]

    fffff8061ec0d337 - nt!IopLiveDumpEstimateMemoryPages+123 (+0x29)

[ ab:b4 ]

    fffff8061ec0d360 - nt!IopLiveDumpEstimateMemoryPages+14c (+0x29)

[ ab:b4 ]

    fffff8061ec0d970 - nt!IopLiveDumpAllocAndInitResources+1e4 (+0x610)

[ a5:ae ]

    fffff8061ec0ea81-fffff8061ec0ea82  2 bytes - nt!MiFilterCrashDumpPte+81 (+0x1111)

[ 00 de:80 8a ]

    fffff8061ec0ea9e-fffff8061ec0ea9f  2 bytes - nt!MiFilterCrashDumpPte+9e (+0x1d)

[ 00 de:80 8a ]

    fffff8061ec0eabc-fffff8061ec0eabd  2 bytes - nt!MiFilterCrashDumpPte+bc (+0x1e)

[ 80 f6:00 89 ]

    fffff8061ec0eb7d-fffff8061ec0eb7e  2 bytes - nt!MiFilterCrashDumpPte+17d (+0xc1)

[ 00 de:80 8a ]

    fffff8061ec0ebf8-fffff8061ec0ebf9  2 bytes - nt!MiFilterCrashDumpPte+1f8 (+0x7b)

[ 80 f6:00 89 ]

    fffff8061ec0efac-fffff8061ec0efad  2 bytes - nt!MmTryIdentifyPage+3c (+0x3b4)

[ 00 de:80 8a ]

    fffff8061ec0efe1-fffff8061ec0efe2  2 bytes - nt!MmTryIdentifyPage+71 (+0x35)

[ 00 de:80 8a ]

    fffff8061ec0f34b - nt!MmRemoveSystemCacheFromDump+23 (+0x36a)

[ 8b:94 ]

    fffff8061ec0ffb2 - nt!MmAddRangeToCrashDump+32 (+0xc67)

[ 7f:88 ]

    fffff8061ec10bb4-fffff8061ec10bb5  2 bytes - nt!MiMirrorRemoveInactivePages+34 (+0xc02)

[ 00 de:80 8a ]

    fffff8061ec10cdb-fffff8061ec10cdc  2 bytes - nt!MiMirrorRemoveInactivePages+15b (+0x127)

[ 00 de:80 8a ]

    fffff8061ec10d5e-fffff8061ec10d5f  2 bytes - nt!MiMirrorRemoveInactivePages+1de (+0x83)

[ 00 de:80 8a ]

    fffff8061ec10f2e-fffff8061ec10f2f  2 bytes - nt!MiGetBaseResidentPageForBugCheck+6 (+0x1d0)

[ 00 de:80 8a ]

    fffff8061ec12219-fffff8061ec1221a  2 bytes - nt!MiBuildReservationCluster+ad (+0x12eb)

[ 00 de:80 8a ]

    fffff8061ec123c3-fffff8061ec123c4  2 bytes - nt!MiBuildReservationCluster+257 (+0x1aa)

[ 00 de:80 8a ]

    fffff8061ec124ac-fffff8061ec124ad  2 bytes - nt!MiBuildReservationCluster+340 (+0xe9)

[ 80 f6:00 89 ]

    fffff8061ec12715-fffff8061ec12716  2 bytes - nt!MiBuildReservationCluster+5a9 (+0x269)

[ 00 de:80 8a ]

    fffff8061ec128db-fffff8061ec128dc  2 bytes - nt!MiGetPageForWriteCluster+47 (+0x1c6)

[ 00 de:80 8a ]

    fffff8061ec12f3c-fffff8061ec12f3d  2 bytes - nt!MiGatherPagefilePages+4bc (+0x661)

[ 00 de:80 8a ]

WARNING: !chkimg output was truncated to 50 lines. Invoke !chkimg without '-lo [num\_lines]' to view  entire output.

    fffff8061f07f63e - nt!CmSaveKey+62

[ 88:91 ]

    fffff8061f07f95b - nt!CmpCreateTemporaryHive+43 (+0x31d)

[ 85:8e ]

    fffff8061f07fa1f - nt!CmpKeyEnumStackStartFromKcbStack+3f (+0xc4)

[ 84:8d ]

    fffff8061f07fdee - nt!CmpEnumerateLayeredKey+66 (+0x3cf)

[ 80:89 ]

    fffff8061f080154 - nt!CmpPromoteSingleKeyFromKcbStacks+4c (+0x366)

[ 7d:86 ]

    fffff8061f08016e - nt!CmpPromoteSingleKeyFromKcbStacks+66 (+0x1a)

[ 7d:86 ]

    fffff8061f0802db - nt!CmpValueEnumStackStartFromKcbStack+3f (+0x16d)

[ 7b:84 ]

    fffff8061f080393 - nt!CmEnumerateValueFromLayeredKey+4b (+0xb8)

[ 7b:84 ]

    fffff8061f0806b6 - nt!CmpGetSubKeyCountForKeyNodeStack+36 (+0x323)

[ 78:81 ]

    fffff8061f080891 - nt!CmpSubtreeEnumeratorStart+6d (+0x1db)

[ 76:7f ]

    fffff8061f080b9b - nt!CmpDoAccessCheckOnLayeredSubtree+4b (+0x30a)

[ 73:7c ]

    fffff8061f080d9e - nt!CmpPromoteSubtree+42 (+0x203)

[ 71:7a ]

    fffff8061f08146b - nt!CmpKeyEnumStackInitialize+17 (+0x6cd)

[ 6a:73 ]

    fffff8061f0818f0 - nt!CmpKeyEnumStackEntryInitialize+1c (+0x485)

[ 65:6e ]

    fffff8061f081d43 - nt!CmpFullPromoteSingleKeyFromKeyNodeStacks+47 (+0x453)

[ 61:6a ]

    fffff8061f082779 - nt!CmpValueEnumStackInitialize+19 (+0xa36)

[ 57:60 ]

    fffff8061f0829ef - nt!CmpSortedValueEnumStackInitialize+27 (+0x276)

[ 54:5d ]

    fffff8061f0843d3 - nt!PiPnpRtlServiceFilterCallback+43 (+0x19e4)

[ 3a:43 ]

    fffff8061f085a78 - nt!MmStoreAllocateVirtualMemory+50 (+0x16a5)

[ 24:2d ]

    fffff8061f085d53 - nt!\_PnpCreateObject+3f (+0x2db)

[ 21:2a ]

    fffff8061f085e5d - nt!\_PnpCreateObjectDispatch+39 (+0x10a)

[ 20:29 ]

    fffff8061f085fcb - nt!ExProcessCounterSetCallback+9b (+0x16e)

[ 1e:27 ]

    fffff8061f085fdc - nt!ExProcessCounterSetCallback+ac (+0x11)

[ 1e:27 ]

    fffff8061f085fee - nt!ExProcessCounterSetCallback+be (+0x12)

[ 1e:27 ]

    fffff8061f086590 - nt!PpmWmiGetAllData+178 (+0x5a2)

[ 19:22 ]

    fffff8061f087205 - nt!WmipQueryAllDataMultiple+7d (+0xc75)

[ 0c:15 ]

    fffff8061f0872d0 - nt!WmipQueryAllDataMultiple+148 (+0xcb)

[ 0b:14 ]

    fffff8061f0880e7-fffff8061f0880e8  2 bytes - nt!\_CmDeleteDevice+37 (+0xe17)

[ fd de:06 df ]

    fffff8061f08845a-fffff8061f08845b  2 bytes - nt!\_CmDeleteDeviceInterfaceRegKey+36 (+0x373)

[ fa de:03 df ]

    fffff8061f088cef - nt!\_CmDeleteDeviceRegKey+3b (+0x895)

[ f1:fa ]

    fffff8061f0897ab - nt!\_CmDeleteDeviceInterface+37 (+0xabc)

[ e7:f0 ]

    fffff8061f0898d7 - nt!\_CmRemoveDeviceFromContainer+3b (+0x12c)

[ e5:ee ]

    fffff8061f08a1e8 - nt!PiCMSetDeviceProblem+44 (+0x911)

[ dc:e5 ]

    fffff8061f08aad6 - nt!PnpQueueQueryAndRemoveEvent+da (+0x8ee)

[ d3:dc ]

    fffff8061f08afb4 - nt!PpDevCfgProcessDeviceReset+3c (+0x4de)

[ cf:d8 ]

    fffff8061f08b62c - nt!PpDevCfgProcessDeviceClass+40 (+0x678)

[ c8:d1 ]

    fffff8061f08be87 - nt!MiAllocatePerSessionProtos+d7 (+0x85b)

[ c0:c9 ]

    fffff8061f08cc88 - nt!SepAdtSecurityDescriptorChangedAuditAlarm+98 (+0xe01)

[ b2:bb ]

    fffff8061f08d48c - nt!AlpcpGetDataFromUserVaSafe+40 (+0x804)

[ aa:b3 ]

    fffff8061f08fcf5 - nt!\_CmSetInstallerClassRegProp+41 (+0x2869)

[ 81:8a ]

    fffff8061f090c83 - nt!CmFcManagerUpdateFeatureUsageSubscriptions+53 (+0xf8e)

[ 72:7b ]

    fffff8061f0917d4 - nt!PiIrpQueryRemoveDevice+4c (+0xb51)

[ 66:6f ]

    fffff8061f091f1b - nt!MiCommitFileBackedSection+e7 (+0x747)

[ 5f:68 ]

    fffff8061f092794 - nt!DbgkRegisterErrorPort+84 (+0x879)

[ 57:60 ]

    fffff8061f092b8a - nt!AlpcpInitializeCompletionList+b6 (+0x3f6)

[ 53:5c ]

    fffff8061f092c7f - nt!AlpcpInitializeCompletionList+1ab (+0xf5)

[ 52:5b ]

    fffff8061f092e48 - nt!AlpcpInitializeCompletionList+374 (+0x1c9)

[ 50:59 ]

    fffff8061f0937ca - nt!KiSynchNumaCounterSetCallback+5a (+0x982)

[ 46:4f ]

    fffff8061f0937d8 - nt!KiSynchNumaCounterSetCallback+68 (+0x0e)

[ 46:4f ]

    fffff8061f09383b - nt!KiSynchNumaCounterSetCallback+cb (+0x63)

[ 46:4f ]

WARNING: !chkimg output was truncated to 50 lines. Invoke !chkimg without '-lo [num\_lines]' to view  entire output.

    fffff8061f4a3cd0 - nt!HaliQuerySystemInformation+40

[ 41:4a ]

    fffff8061f4a607b - nt!HalpMceInitializeErrorPacketContents+13 (+0x23ab)

[ 1e:27 ]

    fffff8061f4a6355 - nt!KiInitializeTopologyStructures+155 (+0x2da)

[ 1b:24 ]

    fffff8061f4a70ff - nt!KiInitializeKernel+ef (+0xdaa)

[ 0d:16 ]

    fffff8061f4a7de0 - nt!PoInitializePrcb+30 (+0xce1)

[ 00:09 ]

    fffff8061f4a8c59 - nt!KiInitializeBootStructures+4b9 (+0xe79)

[ f2:fb ]

    fffff8061f4a9101 - nt!KiInitPrcb+2f5 (+0x4a8)

[ ed:f6 ]

    fffff8061f4a91a0 - nt!KiInitPrcb+394 (+0x9f)

[ ed:f6 ]

    fffff8061f4a9314 - nt!HalpMmBuildTiledMemoryMap+2c (+0x174)

[ eb:f4 ]

    fffff8061f4a93e9 - nt!HalpMapCR3Ex+69 (+0xd5)

[ ea:f3 ]

    fffff8061f4a9526 - nt!EmonCompleteInitializeProfiling+a6 (+0x13d)

[ e9:f2 ]

    fffff8061f4a953f - nt!EmonCompleteInitializeProfiling+bf (+0x19)

[ e9:f2 ]

    fffff8061f4a9bc7 - nt!KiInitializePrcbContext+6f (+0x688)

[ e2:eb ]

    fffff8061f4aa321 - nt!IvtInitializeIommu+261 (+0x75a)

[ db:e4 ]

    fffff8061f4aa4c9 - nt!IvtInitializeIommu+409 (+0x1a8)

[ d9:e2 ]

    fffff8061f4aa6a0 - nt!IvtInitializeIommu+5e0 (+0x1d7)

[ d8:e1 ]

    fffff8061f4aa7aa - nt!IvtInitializeIommu+6ea (+0x10a)

[ d7:e0 ]

    fffff8061f4ab5a1 - nt!KiInitializeXSaveConfiguration+51 (+0xdf7)

[ c9:d2 ]

    fffff8061f4abbe4 - nt!HalpMcaInitializePcrContext+ec (+0x643)

[ c2:cb ]

    fffff8061f4ac566 - nt!HalpPiix4Detect+82 (+0x982)

[ b9:c2 ]

    fffff8061f4ae3da - nt!KeInitThread+ba86 (+0x1e74)

[ 9a:a3 ]

    fffff8061f4afa2a - nt!EmonCompleteInitializeProfiling+65aa (+0x1650)

[ 84:8d ]

    fffff8061f4b0d15 - nt!HalpMcaResumeProcessorConfig+35 (+0x12eb)

[ 71:7a ]

    fffff8061f4b0d52 - nt!HalpMcaResumeProcessorConfig+72 (+0x3d)

[ 71:7a ]

    fffff8061f4b1b13 - nt!HalpBuildResumeStructures+37 (+0xdc1)

[ 63:6c ]

    fffff8061f4b29d4 - nt!HalpCheckLowMemoryPreSleep+ac (+0xec1)

[ 54:5d ]

    fffff8061f4b3ecc - nt!HalpStopLegacyUsbInterruptsInternal+30 (+0x14f8)

[ 3f:48 ]

    fffff8061f4b3fb1 - nt!HalpBlkInitializeIdt+21 (+0xe5)

[ 3f:48 ]

    fffff8061f4b409e - nt!HalpBlkInitializeProcessorState+32 (+0xed)

[ 3e:47 ]

    fffff8061f4b40ae - nt!HalpBlkInitializeProcessorState+42 (+0x10)

[ 3e:47 ]

    fffff8061f4b428c - nt!HalpBlkStartBlockedProcessor+20 (+0x1de)

[ 3c:45 ]

    fffff8061f4b45dc - nt!Amd64InitializeProfiling+24c (+0x350)

[ 38:41 ]

    fffff8061f4b462d - nt!Amd64InitializeProfiling+29d (+0x51)

[ 38:41 ]

    fffff8061f4b4acd - nt!IvtProcessDeviceExceptions+29 (+0x4a0)

[ 33:3c ]

    fffff8061f4b4b40 - nt!IvtProcessDeviceExceptions+9c (+0x73)

[ 33:3c ]

    fffff8061f4b4d97 - nt!HsaInitializeInterruptRemapping+bf (+0x257)

[ 31:3a ]

    fffff8061f4b4f73 - nt!HsaInitializeIommu+103 (+0x1dc)

[ 2f:38 ]

    fffff8061f4b5041 - nt!HsaInitializeIommu+1d1 (+0xce)

[ 2e:37 ]

    fffff8061f4b55ba - nt!HalpIvtpInitializeReservedDomain+72 (+0x579)

[ 29:32 ]

    fffff8061f4b65d5 - nt!PnprQuiesceDevices+31 (+0x101b)

[ 18:21 ]

    fffff8061f4b6be9 - nt!PnprQuiesceProcessors+45 (+0x614)

[ 12:1b ]

    fffff8061f4b70ff - nt!PnprQuiesceWorker+2f (+0x516)

[ 0d:16 ]

    fffff8061f4b73d4 - nt!IoBuildPoDeviceNotifyList+74 (+0x2d5)

[ 0a:13 ]

    fffff8061f4b8772-fffff8061f4b8773  2 bytes - nt!KiUpdateSavedSupervisorState+d6 (+0x139e)

[ f7 9b:00 9c ]

    fffff8061f4b889a - nt!KiInitializeDynamicProcessorDpc+3a (+0x128)

[ f6:ff ]

    fffff8061f4b88ff - nt!KiInitializeDynamicProcessorDpc+9f (+0x65)

[ f5:fe ]

    fffff8061f4bb06e - nt!PopBuildMemoryImageHeader+5a (+0x276f)

[ ce:d7 ]

    fffff8061f4bb42d - nt!PopCompressHiberBlocks+39 (+0x3bf)

[ ca:d3 ]

    fffff8061f4bb82c - nt!PopDecompressHiberBlocks+58 (+0x3ff)

[ c6:cf ]

    fffff8061f4bbe58 - nt!PopEndMirroring+158 (+0x62c)

[ c0:c9 ]

WARNING: !chkimg output was truncated to 50 lines. Invoke !chkimg without '-lo [num\_lines]' to view  entire output.

    fffff8061f4c9363 - nt!KdpReportLoadSymbolsStateChange+53

[ eb:f4 ]

    fffff8061f4c9ed8 - nt!KdpCreateRemoteFile+44 (+0xb75)

[ df:e8 ]

    fffff8061f4ca43e - nt!KdLogDbgPrint+16e (+0x566)

[ da:e3 ]

    fffff8061f4ca496 - nt!KdLogDbgPrint+1c6 (+0x58)

[ da:e3 ]

    fffff8061f4ca5be - nt!HalpRegisterDeviceInUse+7e (+0x128)

[ d8:e1 ]

    fffff8061f4ca739 - nt!KdSendTraceData+51 (+0x17b)

[ d7:e0 ]

    fffff8061f4ca9ee - nt!KdpInitializeExtendedContext+92 (+0x2b5)

[ d4:dd ]

    fffff8061f4cb8b9 - nt!KdpReportExceptionStateChange+51 (+0xecb)

[ c6:cf ]

    fffff8061f4cca6a - nt!HalpKdEnumerateDebuggingDevices+145a (+0x11b1)

[ b4:bd ]

    fffff8061f4ccdd4 - nt!KdpCloseRemoteFile+3c (+0x36a)

[ b0:b9 ]

    fffff8061f4cd043 - nt!KdpReadRemoteFile+43 (+0x26f)

[ ae:b7 ]

    fffff8061f4cd690 - nt!KdpReportCommandStringStateChange+50 (+0x64d)

[ a8:b1 ]

    fffff8061f4cd6ce - nt!KdpReportCommandStringStateChange+8e (+0x3e)

[ a7:b0 ]

    fffff8061f504e1e - nt!AnFwDisplayFade+3ea

[ 30:39 ]

    fffff8061f504e61 - nt!AnFwDisplayFade+42d (+0x43)

[ 30:39 ]

    fffff8061f504fe2 - nt!AnFwDisplayFade+5ae (+0x181)

[ 2e:37 ]

    fffff8061f506087 - nt!BgpFwLibraryInitialize+40f (+0x10a5)

[ 1e:27 ]

    fffff8061f506355 - nt!BgpTxtCreateRegion+a9 (+0x2ce)

[ 1b:24 ]

    fffff8061f50679e - nt!BgpConsoleInitialize+be (+0x449)

[ 17:20 ]

    fffff8061f50ab10 - nt!LogFwInitialize+cc (+0x4372)

[ d3:dc ]

    fffff8061f513011-fffff8061f513013  3 bytes - nt!RtlFunctionOverrideSelfTest$thunk$6746816294339431247+1

[ 33 86 b6:cb db 8f ]

    fffff8061f513022 - nt!memset$thunk$772440563353939046+2 (+0x11)

[ 4e:57 ]

9661 errors : !nt (fffff8061eb506c0-fffff8061f513022)

MODULE\_NAME: memory\_corruption

IMAGE\_NAME:  memory\_corruption

MEMORY\_CORRUPTOR:  LARGE

STACK\_COMMAND:  .cxr; .ecxr ; kb

FAILURE\_BUCKET\_ID:  LKD\_MEMORY\_CORRUPTION\_LARGE

OS\_VERSION:  10.0.25972.1000

BUILDLAB\_STR:  rs\_prerelease

OSPLATFORM\_TYPE:  x64

OSNAME:  Windows 10

FAILURE\_ID\_HASH:  {06247c58-1f9d-5de1-61a8-49cc4ccb24d5}

Followup:     memory\_corruption

---------

[https://hsdes.intel.com/appstore/article/#/22018925397](https://hsdes.intel.com/appstore/article/" \l "/22018925397)

[MTL-P] [GCS] CLOCK\_WATCHDOG\_TIMEOUT\_INVALID\_CONTEXT\_nt!KeAccumulateTicks:

Microsoft (R) Windows Debugger Version 10.0.22621.755 AMD64

Copyright (c) Microsoft Corporation. All rights reserved.

Loading Dump File [C:\DMP\MEMORY\_G05-MTLHG-B1\_2023-10-02\_19-02-45.DMP]

Kernel Bitmap Dump File: Full address space is available

Dump completed successfully, progress percentage: 100

Symbol search path is: srv\*

Executable search path is:

Windows 10 Kernel Version 25967 MP (22 procs) Free x64

Product: WinNt, suite: TerminalServer SingleUserTS

Edition build lab: 25967.1000.amd64fre.rs\_prerelease.230929-1123

Machine Name:

Kernel base = 0xfffff803`6b400000 PsLoadedModuleList = 0xfffff803`6c013d90

Debug session time: Mon Oct  2 09:56:49.182 2023 (UTC - 7:00)

System Uptime: 0 days 0:00:39.901

Loading Kernel Symbols

...............................................................

................................................................

................................................................

......

Loading User Symbols

Loading unloaded module list

...................

For analysis of this file, run !analyze -v

11: kd> !analyze -v

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

\*                                                                             \*

\*                        Bugcheck Analysis                                    \*

\*                                                                             \*

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

CLOCK\_WATCHDOG\_TIMEOUT (101)

An expected clock interrupt was not received on a secondary processor in an

MP system within the allocated interval. This indicates that the specified

processor is hung and not processing interrupts.

Arguments:

Arg1: 0000000000000009, Clock interrupt time out interval in nominal clock ticks.

Arg2: 0000000000000000, 0.

Arg3: ffffd28147726180, The PRCB address of the hung processor.

Arg4: 0000000000000001, The index of the hung processor.

Debugging Details:

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

KEY\_VALUES\_STRING: 1

    Key  : Analysis.CPU.mSec

    Value: 2749

    Key  : Analysis.DebugAnalysisManager

    Value: Create

    Key  : Analysis.Elapsed.mSec

    Value: 2705

    Key  : Analysis.Init.CPU.mSec

    Value: 2905

    Key  : Analysis.Init.Elapsed.mSec

    Value: 56644

    Key  : Analysis.Memory.CommitPeak.Mb

    Value: 89

    Key  : WER.OS.Branch

    Value: rs\_prerelease

    Key  : WER.OS.Timestamp

    Value: 2023-09-29T11:23:00Z

    Key  : WER.OS.Version

    Value: 10.0.25967.1000

FILE\_IN\_CAB:  MEMORY\_G05-MTLHG-B1\_2023-10-02\_19-02-45.DMP

TAG\_NOT\_DEFINED\_202b:  \*\*\* Unknown TAG in analysis list 202b

DUMP\_FILE\_ATTRIBUTES: 0x1800

BUGCHECK\_CODE:  101

BUGCHECK\_P1: 9

BUGCHECK\_P2: 0

BUGCHECK\_P3: ffffd28147726180

BUGCHECK\_P4: 1

FAULTING\_PROCESSOR: 1

PROCESS\_NAME:  lsass.exe

BLACKBOXBSD: 1 (!blackboxbsd)

BLACKBOXNTFS: 1 (!blackboxntfs)

BLACKBOXPNP: 1 (!blackboxpnp)

STACK\_TEXT:

ffffd281`47dd88c8 fffff803`6b8bcb1a     : 00000000`00000101 00000000`00000009 00000000`00000000 ffffd281`47726180 : nt!KeBugCheckEx

ffffd281`47dd88d0 fffff803`6b674624     : 00000000`00000000 00000000`000009f9 00000000`000005f2 ffffd281`47d6b180 : nt!KeAccumulateTicks+0x24773a

ffffd281`47dd8950 fffff803`6b6720dc     : 00000000`00000016 00000000`00000000 ffffd281`47d6b180 00000000`00000900 : nt!KiUpdateRunTime+0xf4

ffffd281`47dd8ac0 fffff803`6b672a55     : 00000000`00000000 ffffd281`47d6b180 00000000`00000246 00000000`00000002 : nt!KiUpdateTime+0x11cc

ffffd281`47dd8d70 fffff803`6b6721ed     : ffffa88a`95f8f370 00000000`00000001 00000000`00000002 fffff803`6c0a0308 : nt!KeClockInterruptNotify+0x405

ffffd281`47dd8f40 fffff803`6b63e54c     : 00000000`17cb872e ffff9301`b7d663e0 ffff9301`b7d66490 fffff803`6b866a5c : nt!HalpTimerClockInterrupt+0xdd

ffffd281`47dd8f70 fffff803`6b866abe     : ffffa88a`95f8f3f0 ffff9301`b7d663e0 fffff803`703e9590 00000000`00000000 : nt!KiCallInterruptServiceRoutine+0x9c

ffffd281`47dd8fb0 fffff803`6b86726c     : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : nt!KiInterruptSubDispatchNoLockNoEtw+0x4e

ffffa88a`95f8f370 fffff803`6b96e070     : 00000000`00000000 00000000`00000000 00000000`00000000 00000001`00000001 : nt!KiInterruptDispatchNoLockNoEtw+0x3c

ffffa88a`95f8f500 fffff803`6b6ac3cf     : 00000027`eb5a16d5 ffff9301`b7d32000 fffff803`703e9580 fffff803`703e9590 : nt!KiConfigureHeteroProcessorsTarget+0x140

ffffa88a`95f8f5b0 fffff803`6b6ab776     : 00000000`00000008 00000000`00000000 ffffd281`47d6b180 00000000`00000000 : nt!KiExecuteAllDpcs+0x55f

ffffa88a`95f8f900 fffff803`6b86599e     : 00000015`b4f26100 ffffd281`47d6b180 00000000`00000000 ffff9301`dca7f180 : nt!KiRetireDpcList+0x366

ffffa88a`95f8fb80 00000000`00000000     : ffffa88a`95f90000 ffffa88a`95f89000 00000000`00000000 00000000`00000000 : nt!KiIdleLoop+0x9e

SYMBOL\_NAME:  nt!KeAccumulateTicks+24773a

MODULE\_NAME: nt

IMAGE\_NAME:  ntkrnlmp.exe

STACK\_COMMAND:  .cxr; .ecxr ; kb

BUCKET\_ID\_FUNC\_OFFSET:  24773a

FAILURE\_BUCKET\_ID:  CLOCK\_WATCHDOG\_TIMEOUT\_INVALID\_CONTEXT\_nt!KeAccumulateTicks

OS\_VERSION:  10.0.25967.1000

BUILDLAB\_STR:  rs\_prerelease

OSPLATFORM\_TYPE:  x64

OSNAME:  Windows 10

FAILURE\_ID\_HASH:  {95498f51-33a9-903b-59e5-d236937d8ecf}

Followup:     MachineOwner

---------

<https://hsdes.intel.com/appstore/article/#/22018875531>

[WS 2022] PAGE\_FAULT\_IN\_NONPAGED\_AREA BSOD observed when using WS 2022 with GHES v2 on GNR and SRF

0: kd> !analyze -v

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

\*                                                                             \*

\*                        Bugcheck Analysis                                    \*

\*                                                                             \*

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

PAGE\_FAULT\_IN\_NONPAGED\_AREA (50)

Invalid system memory was referenced.  This cannot be protected by try-except.

Typically the address is just plain bad or it is pointing at freed memory.

Arguments:

Arg1: ffffd40545c00000, memory referenced.

Arg2: 0000000000000002, value 0 = read operation, 1 = write operation.

Arg3: fffff8015efbe90f, If non-zero, the instruction address which referenced the bad memory

address.

Arg4: 0000000000000002, (reserved)

TRAP\_FRAME:  ffffef0b56607050 -- (.trap 0xffffef0b56607050)

NOTE: The trap frame does not contain all registers.

Some register values may be zeroed or incorrect.

rax=0000000000000300 rbx=0000000000000000 rcx=00000000c4004fcf

rdx=000000000251c71b rsi=0000000000000000 rdi=0000000000000000

rip=fffff8015efbe90f rsp=ffffef0b566071e8 rbp=ffffd4049ec00000

 r8=ffffd4049620e8a0  r9=ffffd40545c00040 r10=000000007eebc480

r11=ffffd4049ec00000 r12=0000000000000000 r13=0000000000000000

r14=0000000000000000 r15=0000000000000000

iopl=0         nv up ei pl nz na po cy

nt!WheapInitializeErrorRecordWrapper+0x6f:

fffff801`5efbe90f 66418941c0      mov     word ptr [r9-40h],ax ds:ffffd405`45c00000=????

Resetting default scope

STACK\_TEXT:

ffffef0b`56606da8 fffff801`5ee0d017     : 00000000`00000050 ffffd405`45c00000 00000000`00000002 ffffef0b`56607050 : nt!KeBugCheckEx

ffffef0b`56606db0 fffff801`5ef3901e     : 0000000f`ffffffff 00000000`00000002 00000000`00000000 ffffd405`45c00000 : nt!MiSystemFault+0xa07

ffffef0b`56606eb0 fffff801`5f02a841     : 00000000`0001e2d0 fffff801`5ef5a7c5 00000000`00000001 ffffef0b`56607141 : nt!MmAccessFault+0x2ee

ffffef0b`56607050 fffff801`5efbe90f     : fffff801`5f410879 ffffd404`9620e8a0 00000000`61656857 00000000`f08a6bb0 : nt!KiPageFault+0x341

ffffef0b`566071e8 fffff801`5f410879     : ffffd404`9620e8a0 00000000`61656857 00000000`f08a6bb0 00000000`00000000 : nt!WheapInitializeErrorRecordWrapper+0x6f

ffffef0b`566071f0 fffff801`5f6de438     : ffffd404`9620e8a0 00000000`00000008 00000000`00000000 00000000`00000000 : nt!WheapInitializeErrorSource+0xb5

ffffef0b`56607230 fffff801`5f6de8ee     : ffffd404`8d8b0300 ffffef0b`566072c8 ffffd404`8d8b09a0 00000000`00000001 : nt!WheapInitializeErrorSourceTable+0x110

ffffef0b`56607260 fffff801`5f6de087     : fffff801`59257140 fffff801`00000009 00000000`00000000 00000000`00000000 : nt!WheaInitialize+0x45a

ffffef0b`56607310 fffff801`5f6fc865     : fffff801`5ab1c000 fffff801`59257140 fffff801`5f433420 fffff801`59257100 : nt!IoInitSystemPreDrivers+0xcf3

ffffef0b`56607450 fffff801`5f43345b     : fffff801`59257140 fffff801`5f8527c8 fffff801`5f433420 fffff801`59257140 : nt!IoInitSystem+0x15

ffffef0b`56607480 fffff801`5eec8785     : ffffd404`8d8b0300 fffff801`5f433420 fffff801`59257140 00000000`00000000 : nt!Phase1Initialization+0x3b

ffffef0b`566074b0 fffff801`5f01ed48     : fffff801`5aa0d180 ffffd404`8d8b0300 fffff801`5eec8730 00000000`00000000 : nt!PspSystemThreadStartup+0x55

ffffef0b`56607500 00000000`00000000     : ffffef0b`56608000 ffffef0b`56601000 00000000`00000000 00000000`00000000 : nt!KiStartSystemThread+0x28

0: kd> !pool ffffd40545c00000

Pool page ffffd40545c00000 region is Nonpaged pool

ffffd40545c00000 is not a valid large pool allocation, checking large session pool...

Unable to read large session pool table (Session data is not present in mini and kernel-only dumps)

ffffd40545c00000 is not valid pool. Checking for freed (or corrupt) pool

Address ffffd40545c00000 could not be read. It may be a freed, invalid or paged out page

0: kd> u nt!WheapInitializeErrorSource+0xa8

nt!WheapInitializeErrorSource+0xa8:

fffff801`5f41086c 4c8bc3          mov     r8,rbx

fffff801`5f41086f 8bd6            mov     edx,esi

fffff801`5f410871 498bcb          mov     rcx,r11

fffff801`5f410874 e827e0baff      call    nt!WheapInitializeErrorRecordWrapper (fffff801`5efbe8a0)

fffff801`5f410879 4d03df          add     r11,r15

fffff801`5f41087c 41ffc6          inc     r14d

fffff801`5f41087f 443b731c        cmp     r14d,dword ptr [rbx+1Ch]

fffff801`5f410883 72e7            jb      nt!WheapInitializeErrorSource+0xa8 (fffff801`5f41086c)

0: kd> .frame /r 5

05 ffffef0b`566071f0 fffff801`5f6de438     nt!WheapInitializeErrorSource+0xb5

rax=0000000000000300 rbx=ffffd4049620e8a0 rcx=00000000c4004fcf

rdx=000000000251c71b rsi=00000000f08a6bb0 rdi=0000000000000000

rip=fffff8015f410879 rsp=ffffef0b566071f0 rbp=ffffd4049ec00000

 r8=ffffd4049620e8a0  r9=ffffd40545c00040 r10=000000007eebc480

r11=ffffd4049ec00000 r12=fffff80159257140 r13=0000000000000001

r14=0000000000000000 r15=00000000f08a6bb0

iopl=0         nv up ei pl zr na po nc

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

nt!WheapInitializeErrorSource+0xb5:

fffff801`5f410879 4d03df          add     r11,r15

0: kd> !pool ffffd4049ec00000

Pool page ffffd4049ec00000 region is Nonpaged pool

\*ffffd4049ec00000 : large page allocation, tag is Whea, size is 0xa6ee5000 bytes

Owning component : Unknown (update pooltag.txt)

**Business Justification :**

The issue is extremely critical as it is not possible to boot Windows Server OS on the latest Intel platforms.  Without the bug fix ported to WS 2022, validation of GNR and SRF platforms cannot be accomplished on Windows.  This issue will affect enterprise customers as well.

<https://hsdes.intel.com/appstore/article/#/14019074645>

Windows Bugcheck 0x13A observed when Emergency Management Services (EMS) is enabled in boot entry:

IopAllocateLegacyBootResources frees Boot resources for IopInitHalDeviceNode twice – first as IopInitHalDeviceNode->BootResources and then same address as remainingList.

Also, since remainingList is used in the call to IopCombineCmResourceList \***after**\* IopInitHalDeviceNode->BootResources has been freed, there is use-after-free bug there too.

Basically, the newly added check and call to free IopInitHalDeviceNode->BootResources introduces two bugs – use-after-free and double-free:

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

**KERNEL\_MODE\_HEAP\_CORRUPTION (13a)**

**The kernel mode heap manager has detected corruption in a heap.**

**Arguments:**

**Arg1: 0000000000000011, Type of corruption detected**

**Arg2: ffff87823b600180, Address of the heap that reported the corruption**

**Arg3: ffff87823cc81100, Address at which the corruption was detected**

**Arg4: 0000000000000000**

**18: kd> !pool ffff87823cc81100**

**MAX\_SYSTEM\_VA\_ASSIGNMENTS needs to be increased**

**Pool page ffff87823cc81100 region is Paged pool**

**…**

**\*ffff87823cc81100 size:   40 previous size:    0  (Free)      \*Pp**

**…**

**18: kd> k**

**# Child-SP          RetAddr               Call Site**

**00 fffff484`60c066c8 fffff801`08bb70c2     nt!DbgBreakPointWithStatus**

**01 fffff484`60c066d0 fffff801`08bb6864     nt!KiBugCheckDebugBreak+0x12**

**02 fffff484`60c06730 fffff801`08a3fbb7     nt!KeBugCheck2+0xc04**

**03 fffff484`60c06eb0 fffff801`08c01e78     nt!KeBugCheckEx+0x107**

**04 fffff484`60c06ef0 fffff801`08c01ed8     nt!RtlpHeapHandleError+0x40**

**05 fffff484`60c06f30 fffff801`08c01af5     nt!RtlpHpHeapHandleError+0x58**

**06 fffff484`60c06f60 fffff801`08b3fc02     nt!RtlpLogHeapFailure+0x45**

**07 (Inline Function) --------`--------     nt!RtlpHpLfhReportError+0x20**

**08 fffff484`60c06f90 fffff801`089940b5     nt!RtlpHpLfhSubsegmentFreeBlock+0x180bb2**

**09 (Inline Function) --------`--------     nt!RtlpHpLfhContextFree+0x9**

**0a (Inline Function) --------`--------     nt!RtlpHpSegFree+0x11c**

**0b (Inline Function) --------`--------     nt!RtlpHpFreeHeap+0x23f**

**0c fffff484`60c07020 fffff801`09106a85     nt!ExFreeHeapPool+0x965**

**0d fffff484`60c070f0 fffff801`091d1074     nt!ExFreePoolWithTag+0x25**

**0e fffff484`60c07130 fffff801`091a1fb4     nt!IopAllocateLegacyBootResources+0xe4**

**0f fffff484`60c07170 fffff801`091b5600     nt!IopInitializeBootDrivers+0x640**

**10 fffff484`60c07320 fffff801`091ac23f     nt!IoInitSystemPreDrivers+0xbf4**

**11 fffff484`60c07440 fffff801`08eb4afb     nt!IoInitSystem+0x17**

**12 fffff484`60c07470 fffff801`08934297     nt!Phase1Initialization+0x3b**

**13 fffff484`60c074b0 fffff801`08a90234     nt!PspSystemThreadStartup+0x57**

**14 fffff484`60c07500 00000000`00000000     nt!KiStartSystemThread+0x34**

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

**0e fffff484`60c07130 fffff801`091a1fb4     nt!IopAllocateLegacyBootResources+0xe4**

**rax=0000000000000000 rbx=ffff87823cc81110 rcx=0000000000000003**

**rdx=000000000000008a rsi=fffff80105b75860 rdi=ffff87823c46d620**

**rip=fffff801091d1074 rsp=fffff48460c07130 rbp=0000000000000000**

**r8=0000000000000065  r9=0000000000000000 r10=0000000000000000**

**r11=0000000000000000 r12=0000000000000030 r13=ffffc28227bcce40**

**r14=0000000000000000 r15=0000000000000003**

**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!IopAllocateLegacyBootResources+0xe4:**

**fffff801`091d1074 33ff            xor     edi,edi**

**18: kd> ub**

**nt!IopAllocateLegacyBootResources+0xc2:**

**fffff801`091d1052 e895d5d0ff      call    nt!IopCombineCmResourceList (fffff801`08ede5ec)**

**fffff801`091d1057 488b1522c63b00  mov     rdx,qword ptr [nt!IopInitHalDeviceNode (fffff801`0958d680)]**

**fffff801`091d105e 48898220020000  mov     qword ptr [rdx+220h],rax**

**fffff801`091d1065 4885db          test    rbx,rbx**

**fffff801`091d1068 740a            je      nt!IopAllocateLegacyBootResources+0xe4 (fffff801`091d1074)**

**fffff801`091d106a 33d2            xor     edx,edx**

**fffff801`091d106c 488bcb          mov     rcx,rbx**

**fffff801`091d106f e8ec59f3ff      call    nt!ExFreePoolWithTag (fffff801`09106a60)**

**18: kd> !verifier 80 ffff87823cc81110 2**

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

**There are up to 0x40000 entries in the log.**

**Parsing 0x0000000000040000 log entries, searching for address 0xffff87823cc81110.**

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

**Pool block ffff87823cc81110, Size 0000000000000040, Thread ffffc28227724080**

**fffff80109122f48 nt!VfPtFreePoolNotification+0x5c**

**fffff80108993b8b nt!ExFreeHeapPool+0x43b**

**fffff80109106a85 nt!ExFreePoolWithTag+0x25**

**fffff801091d1074 nt!IopAllocateLegacyBootResources+0xe4**

**fffff801091a1fb4 nt!IopInitializeBootDrivers+0x640**

**fffff801091b5600 nt!IoInitSystemPreDrivers+0xbf4**

**fffff801091ac23f nt!IoInitSystem+0x17**

**fffff80108eb4afb nt!Phase1Initialization+0x3b**

**fffff80108934297 nt!PspSystemThreadStartup+0x57**

**fffff80108a90234 nt!KiStartSystemThread+0x34**

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

**Pool block ffff87823cc81110, Size 0000000000000040, Thread ffffc28227724080**

**fffff80109122f48 nt!VfPtFreePoolNotification+0x5c**

**fffff80108993b8b nt!ExFreeHeapPool+0x43b**

**fffff80109106a85 nt!ExFreePoolWithTag+0x25**

**fffff801091d104c nt!IopAllocateLegacyBootResources+0xbc**

**fffff801091a1fb4 nt!IopInitializeBootDrivers+0x640**

**fffff801091b5600 nt!IoInitSystemPreDrivers+0xbf4**

**fffff801091ac23f nt!IoInitSystem+0x17**

**fffff80108eb4afb nt!Phase1Initialization+0x3b**

**fffff80108934297 nt!PspSystemThreadStartup+0x57**

**fffff80108a90234 nt!KiStartSystemThread+0x34**

**Parsed 0000000000000002 entries out of 0000000000040000.**

**nt!IopAllocateLegacyBootResources+0x6b:**

**fffff801`091d0ffb 488b0d7ec63b00  mov     rcx,qword ptr [nt!IopInitHalDeviceNode (fffff801`0958d680)]**

**fffff801`091d1002 ba40000000      mov     edx,40h**

**fffff801`091d1007 48891d6ac63b00  mov     qword ptr [nt!IopInitHalResources (fffff801`0958d678)],rbx**

**fffff801`091d100e 488b9920020000  mov     rbx,qword ptr [rcx+220h]  çççççççççççççççççç**IopInitHalDeviceNode->BootResources

**fffff801`091d1015 e88a8ab1ff      call    nt!PipSetDevNodeFlags (fffff801`08ce9aa4)**

**fffff801`091d101a 488b155fc63b00  mov     rdx,qword ptr [nt!IopInitHalDeviceNode (fffff801`0958d680)]**

**fffff801`091d1021 4c8bc7          mov     r8,rdi**

**fffff801`091d1024 b901000000      mov     ecx,1**

**fffff801`091d1029 488b5220        mov     rdx,qword ptr [rdx+20h]**

**fffff801`091d102d e85e0ab5ff      call    nt!IopAllocateBootResources (fffff801`08d21a90)**

**fffff801`091d1032 488b0547c63b00  mov     rax,qword ptr [nt!IopInitHalDeviceNode (fffff801`0958d680)]**

**fffff801`091d1039 488b8820020000  mov     rcx,qword ptr [rax+220h]   çççççççççççççççççç**IopInitHalDeviceNode->BootResources

**fffff801`091d1040 4885c9          test    rcx,rcx**

**fffff801`091d1043 7407            je      nt!IopAllocateLegacyBootResources+0xbc (fffff801`091d104c)  Branch**

**nt!IopAllocateLegacyBootResources+0xb5:**

**fffff801`091d1045 33d2            xor     edx,edx**

**fffff801`091d1047 e8145af3ff      call    nt!ExFreePoolWithTag (fffff801`09106a60)**

**nt!IopAllocateLegacyBootResources+0xbc:**

**fffff801`091d104c 488bd7          mov     rdx,rdi**

**fffff801`091d104f 488bcb          mov     rcx,rbx      çççççççççççççççççç**This has been freed already

**fffff801`091d1052 e895d5d0ff      call    nt!IopCombineCmResourceList (fffff801`08ede5ec)**

**fffff801`091d1057 488b1522c63b00  mov     rdx,qword ptr [nt!IopInitHalDeviceNode (fffff801`0958d680)]**

**fffff801`091d105e 48898220020000  mov     qword ptr [rdx+220h],rax**

**fffff801`091d1065 4885db          test    rbx,rbx**

**fffff801`091d1068 740a            je      nt!IopAllocateLegacyBootResources+0xe4 (fffff801`091d1074)  Branch**

**nt!IopAllocateLegacyBootResources+0xda:**

**fffff801`091d106a 33d2            xor     edx,edx**

**fffff801`091d106c 488bcb          mov     rcx,rbx     çççççççççççççççççç**This has been freed already

**fffff801`091d106f e8ec59f3ff      call    nt!ExFreePoolWithTag (fffff801`09106a60)**

<https://hsdes.intel.com/appstore/article/#/22017004021>

[CU][RPL-S]RPL-S\_S-3\_25326\_AV\_VRF\_W\_(null)\_afd!AfdCloseCore:

 AFD.SYS tries to dereference connection which has been freed already:

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

**PAGE\_FAULT\_IN\_NONPAGED\_AREA (50)**

**Invalid system memory was referenced.  This cannot be protected by try-except.**

**Typically the address is just plain bad or it is pointing at freed memory.**

**Arguments:**

**Arg1: ffffbd05fc882f30, memory referenced.**

**Arg2: 0000000000000002, X64: bit 0 set if the fault was due to a not-present PTE.**

**bit 1 is set if the fault was due to a write, clear if a read.**

**bit 3 is set if the processor decided the fault was due to a corrupted PTE.**

**bit 4 is set if the fault was due to attempted execute of a no-execute PTE.**

**- ARM64: bit 1 is set if the fault was due to a write, clear if a read.**

**bit 3 is set if the fault was due to attempted execute of a no-execute PTE.**

**Arg3: fffff8077ce0365e, If non-zero, the instruction address which referenced the bad memory**

**address.**

**Arg4: 0000000000000002, (reserved)**

**8: kd> u fffff8077ce0365e L1**

**afd!AfdCloseCore+0x8e:**

**fffff807`7ce0365e f00fc14730      lock xadd dword ptr [rdi+30h],eax**

**8: kd> r cr2**

**cr2=ffffbd05fc882f30**

**8: kd> !pte ffffbd05fc882f30**

**VA ffffbd05fc882f30**

**PXE at FFFF93C9E4F27BD0    PPE at FFFF93C9E4F7A0B8    PDE at FFFF93C9EF417F20    PTE at FFFF93DE82FE4410**

**contains 0A00000127BD7863  contains 0A00000127BDA863  contains 0A000008969EA863  contains 0000000000000000**

**pfn 127bd7    ---DA--KWEV  pfn 127bda    ---DA--KWEV  pfn 8969ea    ---DA--KWEV  not valid**

**8: kd> !verifier 80 ffffbd05fc882f30-30 1**

**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 0xffffbd05fc882f00.**

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

**Pool block ffffbd05fc882f00, Size 0000000000000100, Thread ffffbd0625f61080**

**fffff8004471ff58 nt!VfPtFreePoolNotification+0x5c**

**fffff8004410d5c3 nt!ExpFreePoolChecks+0x1b08eb**

**fffff8004424edea nt!ExpFreeHeapSpecialPool+0xce**

**fffff8004407b99f nt!ExFreeHeapPool+0x265e1f**

**fffff80044703775 nt!ExFreePoolWithTag+0x25**

**fffff80044217938 nt!DifExFreePoolWrapper+0x88**

**fffff8004471419e nt!VerifierExFreePool+0x3e**

**fffff800447141b9 nt!VerifierExFreePoolEx+0x9**

**fffff80043ea401d nt!ExFreeToLookasideListEx+0xbd**

**fffff8077cdb2c25 afd!PplpGenericFreeFunction+0x15**

**fffff80043ea401d nt!ExFreeToLookasideListEx+0xbd**

**fffff8077cda1bcf afd!AfdFreeConnectionEx+0x63**

**fffff8077cda1813 afd!AfdTLCloseConnectionHandleComplete+0x13**

**fffff8077cd8b669 afunix!AfUnixEndpointDereference+0x1b1**

**fffff8077cd8a16b afunix!AfUnixTlConnectEndpointClose+0xbb**

**fffff8077cda18a6 afd!AfdCloseConnection+0x86**

**fffff8077cdc1cd2 afd!AfdCleanupCore+0x1d6ea**

**fffff8077cda4df5 afd!AfdCleanup+0x3d**

**fffff8077cda55fc afd!AfdDispatch+0xbc**

**fffff80044003b69 nt!IopfCallDriver+0x55**

**fffff800447154a2 nt!IovCallDriver+0x232**

**fffff80043e12535 nt!IofCallDriver+0x85**

**fffff800443502a6 nt!IopCloseFile+0x1a6**

**fffff80044348e46 nt!ObpCloseHandle+0x2c6**

**fffff8004434a449 nt!NtClose+0x39**

**fffff80044069505 nt!KiSystemServiceCopyEnd+0x25**

**Parsed 000000000000000b entries out of 0000000000020000.**

**8: kd> !thread**

**THREAD ffffbd0625f61080  Cid 1418.21a4  Teb: 0000006024113000 Win32Thread: 0000000000000000 RUNNING on processor 8**

**IRP List:**

**ffffbd0618ecad80: (0006,0280) Flags: 40000404  Mdl: 00000000**

**Not impersonating**

**DeviceMap                 ffffce899c584d10**

**Owning Process            ffffbd061c597080       Image:         WUDFHost.exe**

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

**Wait Start TickCount      246077         Ticks: 0**

**Context Switch Count      17031          IdealProcessor: 8**

**UserTime                  00:00:00.359**

**KernelTime                00:01:10.546**

**Win32 Start Address ipfsrv!thread\_wrapper (0x00007ffd63f04150)**

**Stack Init ffffbb09f5617bb0 Current ffffbb09f5616f40**

**Base ffffbb09f5618000 Limit ffffbb09f5611000 Call 0000000000000000**

**Priority 15 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5**

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

**ffffbb09`f56169f8 fffff800`441b1752     : 00000000`00000000 fffff800`43f20530 ffffe501`4541f180 ffffbb09`f5616b60 : nt!DbgBreakPointWithStatus**

**ffffbb09`f5616a00 fffff800`441b0ef4     : ffffe501`00000003 ffffbb09`f5616b60 fffff800`4406eaf0 ffffbb09`f5617110 : nt!KiBugCheckDebugBreak+0x12**

**ffffbb09`f5616a60 fffff800`44007d67     : 00000000`00000000 00000000`00000000 00000000`00000000 ffffbd05`fc882f30 : nt!KeBugCheck2+0xc04**

**ffffbb09`f56171e0 fffff800`440e4a6a     : 00000000`00000050 ffffbd05`fc882f30 00000000`00000002 ffffbb09`f56174b0 : nt!KeBugCheckEx+0x107**

**ffffbb09`f5617220 fffff800`43e3fb81     : 00000000`00000000 ffff8000`00000000 ffffbb09`f5617530 ffffbd05`fc882f30 : nt!MiSystemFault+0x20d6ca**

**ffffbb09`f5617330 fffff800`440651ba     : 00000000`00000000 00000000`00000000 ffffbd06`218f3240 fffff800`4471738d : nt!MmAccessFault+0x421**

**ffffbb09`f56174b0 fffff807`7ce0365e     : ffffbb09`f5617699 ffffbd06`18ecad80 ffffbd06`218f3240 fffff800`443504cc : nt!KiPageFault+0x37a (TrapFrame @ ffffbb09`f56174b0)**

**ffffbb09`f5617640 fffff807`7ce036bd     : ffffbd05`ffe78e20 ffffbd06`218f3240 ffffbd05`fdf15ec8 ffffbd05`ffe78e20 : afd!AfdCloseCore+0x8e**

**ffffbb09`f5617680 fffff807`7cda55b5     : ffffbd06`18ecad80 00000000`00000000 ffffbd05`f3e66ab0 ffffbd06`1c597080 : afd!AfdClose+0x39**

**ffffbb09`f56176b0 fffff800`44003b69     : ffffbd06`18ecad80 ffffbd05`f3e66ab0 ffffbd06`1a4bd4f0 ffffbd05`00000001 : afd!AfdDispatch+0x75**

**ffffbb09`f56176f0 fffff800`447154a2     : ffffbd06`18ecad80 ffffbd05`f3e66ab0 00000000`00000000 fffff800`4407b854 : nt!IopfCallDriver+0x55**

**ffffbb09`f5617730 fffff800`43e12535     : ffffbd06`3446dd60 ffffbb09`f5617900 fffff800`43ed3402 ffffbd06`1a4bd4f0 : nt!IovCallDriver+0x232**

**ffffbb09`f5617770 fffff800`443504cc     : ffffbd06`3446dd60 ffffbb09`f5617989 00000000`00000000 ffffbd06`18ecad80 : nt!IofCallDriver+0x85**

**ffffbb09`f56177b0 fffff800`442ed87e     : ffffbd05`d178ad20 00000000`00000000 ffffbd06`3446dd30 ffffbb09`f5617989 : nt!IopDeleteFile+0x13c**

**ffffbb09`f5617830 fffff800`43e15563     : 00000000`00000000 00000000`00000000 ffffbb09`f5617989 ffffbd06`3446dd60 : nt!ObpRemoveObjectRoutine+0x7e**

**ffffbb09`f5617890 fffff800`44348e9e     : 00000000`00000001 ffffbd06`3446dd30 ffffbb09`f5617989 ffffbd06`3446dd30 : nt!ObfDereferenceObjectWithTag+0xc3**

**(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : nt!ObCloseHandleTableEntry+0x24d (Inline Function @ fffff800`44348e9e)**

**ffffbb09`f56178d0 fffff800`4434a449     : fffff800`4406a945 fffff800`4406a945 00000000`000007d4 fffff800`4406a945 : nt!ObpCloseHandle+0x31e**

**ffffbb09`f56179f0 fffff800`44069505     : ffffbd06`25f61080 00000000`58adfc08 ffffbb09`f5617a38 00000000`00000000 : nt!NtClose+0x39**

**ffffbb09`f5617a20 00007ffd`91e2fdc4     : 00007ffd`8e49650f 00000174`153bda90 00000000`00000001 00000000`00000000 : nt!KiSystemServiceCopyEnd+0x25 (TrapFrame @ ffffbb09`f5617a20)**

**00000060`24c7ed68 00007ffd`8e49650f     : 00000174`153bda90 00000000`00000001 00000000`00000000 00000174`153bdb70 : ntdll!ZwClose+0x14**

**00000060`24c7ed70 00007ffd`8e495288     : 00000174`151c57e0 00000174`153bda90 00000000`000007d4 00007ffd`91104c27 : mswsock!SockCloseSocket+0x15f**

**00000060`24c7ee40 00007ffd`910e67f3     : 00000174`151c57e0 00000000`000007d4 00000174`151ca310 00000000`00000000 : mswsock!WSPCloseSocket+0x78**

**(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : WS2\_32!DPROVIDER::WSPCloseSocket+0x20 (Inline Function @ 00007ffd`910e67f3)**

**00000060`24c7ee90 00007ffd`63f01e50     : 00000000`00000000 00000000`00000000 00000060`24c7f010 00000174`152cfb70 : WS2\_32!closesocket+0x133**

**(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : ipfsrv!esif\_ccb\_socket\_close+0x21 (Inline Function @ 00007ffd`63f01e50)**

**00000060`24c7ef10 00007ffd`63f02c44     : 00000000`00000000 00000174`152ce880 00000000`00000000 00000000`00000000 : ipfsrv!WebServer\_Main+0xab0**

**00000060`24c7f790 00007ffd`63f04170     : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : ipfsrv!WebServer\_WorkerThread+0x44**

**00000060`24c7f7d0 00007ffd`8fbd3e2d     : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : ipfsrv!thread\_wrapper+0x20**

**00000060`24c7f800 00007ffd`91ddf298     : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : KERNEL32!BaseThreadInitThunk+0x1d**

**00000060`24c7f830 00000000`00000000     : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : ntdll!RtlUserThreadStart+0x28**

<https://hsdes.intel.com/appstore/article/#/14018978015>

(WIFI-294183)[WIN11][SV1][WDI] 0x9F - tcpip!FlUnbindAdapter:

TCPIP is waiting for WolOperationsCompleteEvent but no WOL operations appear to be in progress:

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

**DRIVER\_POWER\_STATE\_FAILURE (9f)**

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

**Arguments:**

**Arg1: 0000000000000004, The power transition timed out waiting to synchronize with the Pnp**

**subsystem.**

**Arg2: 000000000000012c, Timeout in seconds.**

**Arg3: ffffd98f54397040, The thread currently holding on to the Pnp lock.**

**Arg4: fffffb8f556ff700, nt!TRIAGE\_9F\_PNP on Win7 and higher**

**14: kd> .thread /p /r ffffd98f54397040**

**Implicit thread is now ffffd98f`54397040**

**…**

**14: kd> !thread ffffd98f54397040**

**THREAD ffffd98f54397040  Cid 0004.8600  Teb: 0000000000000000 Win32Thread: 0000000000000000 WAIT: (UserRequest) KernelMode Non-Alertable**

**ffffd98f4f030ae8  SynchronizationEvent**

**IRP List:**

**ffffd98f74d3c010: (0006,0430) Flags: 00000000  Mdl: 00000000**

**Not impersonating**

**DeviceMap                 ffff92013ae93ea0**

**Owning Process            ffffd98f27ae0040       Image:         System**

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

**Wait Start TickCount      33849744       Ticks: 19201 (0:00:05:00.015)**

**Context Switch Count      37297          IdealProcessor: 9  NoStackSwap**

**UserTime                  00:00:00.000**

**KernelTime                00:00:00.968**

**Win32 Start Address nt!ExpWorkerThread (0xfffff8074608f9a0)**

**Stack Init fffffb8f5d29ab70 Current fffffb8f5d2995b0**

**Base fffffb8f5d29b000 Limit fffffb8f5d294000 Call 0000000000000000**

**Priority 15 BasePriority 12 PriorityDecrement 0 IoPriority 2 PagePriority 5**

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

**fffffb8f`5d2995f0 fffff807`460702b7     : ffffc601`1adc0180 00000000`ffffffff 00000000`00000000 ffffd98f`00000000 : nt!KiSwapContext+0x76**

**fffffb8f`5d299730 fffff807`46072169     : ffffd98f`0000000c 00000000`0000000b fffffb8f`5d299910 00000000`00000000 : nt!KiSwapThread+0x3a7**

**fffffb8f`5d299810 fffff807`4606c084     : 00000000`00000000 fffff807`00000000 fffffb8f`00000000 00000000`00000000 : nt!KiCommitThreadWait+0x159**

**fffffb8f`5d2998b0 fffff807`49b231fa     : ffffd98f`4f030ae8 ffffd98f`00000006 00000000`00000000 fffff807`49c1ca00 : nt!KeWaitForSingleObject+0x234**

**fffffb8f`5d2999a0 fffff807`497e52b6     : fffffb8f`5d299bf0 fffffb8f`5d299c70 ffffd98f`2e7ba8e0 ffffd98f`4ed20aa0 : tcpip!FlUnbindAdapter+0x8827a**

**fffffb8f`5d299b20 fffff807`4981be95     : ffffd98f`67afdd10 ffffd98f`2e7ba8e0 ffffd98f`4ed20aa0 ffffd98f`44c5a1a0 : ndis!ndisInvokeUnbindAdapter+0x72**

**fffffb8f`5d299b70 fffff807`497e4413     : ffff9201`00000000 fffff807`00000001 ffffd98f`67afdd10 ffffffff`ffffffff : ndis!ndisUnbindProtocolOpen+0x225**

**fffffb8f`5d299cd0 fffff807`497e7f4b     : 00000000`00000000 fffffb8f`5d299e20 ffffd98f`44c5a1a0 ffffd98f`44c5b598 : ndis!ndisUnbindEachProtocolOpenOnMiniport+0xcb**

**(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : ndis!ndisUnbindProtocol+0x22 (Inline Function @ fffff807`497e7f4b)**

**fffffb8f`5d299d20 fffff807`497e7644     : ffffd98f`44c5a1a0 ffffd98f`44c5a1a0 ffffd98f`44c5b610 ffffd98f`44c5b598 : ndis!Ndis::BindEngine::Iterate+0x637**

**fffffb8f`5d299ea0 fffff807`497ebda6     : ffffd98f`44c5b598 fffffb8f`5d29a000 00000000`00000000 fffff807`497e8195 : ndis!Ndis::BindEngine::UpdateBindings+0x98**

**fffffb8f`5d299ef0 fffff807`497ebca0     : ffffd98f`44c5b598 00000000`00000000 ffffd98f`44c5a101 fffff807`497e80d7 : ndis!Ndis::BindEngine::DispatchPendingWork+0x76**

**fffffb8f`5d299f20 fffff807`497ebbf6     : ffffd98f`44c5b598 fffffb8f`5d29a000 00000000`00001000 fffff807`497e80d7 : ndis!Ndis::BindEngine::ApplyBindChanges+0x54**

**fffffb8f`5d299f70 fffff807`498278ae     : ffffd98f`44c5a1a0 fffffb8f`5d29a0c0 ffffd98f`44c5b598 ffffd98f`4426f8b0 : ndis!ndisMSetMiniportReadyForBinding+0x8a**

**fffffb8f`5d299fc0 fffff807`4975a453     : ffffd98f`44c5a1a0 ffffd98f`44c5a1a0 00000000`00000000 fffff807`497cb050 : ndis!ndisPnPRemoveDevice+0x31e**

**fffffb8f`5d29a200 fffff807`4980a05c     : ffffd98f`44c5a1a0 ffffd98f`44c5a050 00000000`00000000 fffffb8f`5d29a300 : ndis!ndisPnPRemoveDeviceEx+0x13f**

**fffffb8f`5d29a250 fffff807`49721d86     : ffffd98f`74d3c010 fffffb8f`5d29a300 00000000`00000000 ffffd98f`44c5a1a0 : ndis!ndisPnPIrpRemoveDevice+0x118**

**fffffb8f`5d29a2c0 fffff807`46042a65     : ffffd98f`448b3d01 fffffb8f`5d29a480 00000001`08060001 ffffd98f`2e7bd8b0 : ndis!ndisPnPDispatch+0x17d86**

**(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : nt!IopfCallDriver+0x40 (Inline Function @ fffff807`46042a65)**

**fffffb8f`5d29a330 fffff807`4808974a     : fffffb8f`5d29a480 ffffd98f`2e7bd8b0 00000000`00000000 00000000`00000001 : nt!IofCallDriver+0x55**

**(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : Wdf01000!FxIrp::CallDriver+0x16 (Inline Function @ fffff807`4808974a)**

**fffffb8f`5d29a370 fffff807`48088a4b     : 00000000`00000001 fffffb8f`00000000 ffffd98f`2e7bd800 fffffb8f`5d29a400 : Wdf01000!FxPkgFdo::ProcessRemoveDeviceOverload+0x8a**

**fffffb8f`5d29a3a0 fffff807`4800b459     : ffffd98f`2e7bd8b0 00000000`00000000 00000000`00000000 ffffd98f`515d8350 : Wdf01000!FxPkgPnp::\_PnpRemoveDevice+0x11b**

**fffffb8f`5d29a410 fffff807`48003d83     : ffffd98f`74d3c010 ffffd98f`74d3c010 fffffb8f`5d29a5e0 00000000`00000000 : Wdf01000!FxPkgPnp::Dispatch+0xd9**

**(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : Wdf01000!DispatchWorker+0xfa (Inline Function @ fffff807`48003d83)**

**(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : Wdf01000!FxDevice::Dispatch+0x11b (Inline Function @ fffff807`48003d83)**

**fffffb8f`5d29a480 fffff807`46042a65     : ffff9201`62d4aed0 00000000`00000000 00000000`c00000bb 00000000`69706e04 : Wdf01000!FxDevice::DispatchWithLock+0x153**

**(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : nt!IopfCallDriver+0x40 (Inline Function @ fffff807`46042a65)**

**fffffb8f`5d29a4f0 fffff807`464c3c84     : 00000000`00000002 ffffd98f`448b3de0 00000000`00000000 ffff9201`411734a0 : nt!IofCallDriver+0x55**

**fffffb8f`5d29a530 fffff807`464c9c50     : 00000000`00000002 ffffd98f`2a7bf060 ffffd98f`2a7bfa20 ffffd98f`2a7bf060 : nt!IopSynchronousCall+0xf8**

**fffffb8f`5d29a5a0 fffff807`460ae309     : ffff9201`55bd1630 ffffd98f`2a7bfa20 00000000`00000200 00000000`0000000a : nt!IopRemoveDevice+0x108**

**fffffb8f`5d29a650 fffff807`464cab72     : ffffd98f`2a7bfa20 00000000`00000015 00000000`00000000 cb3a4008`00200001 : nt!PnpRemoveLockedDeviceNode+0x1a9**

**fffffb8f`5d29a6b0 fffff807`464ca8d7     : ffffd98f`2a7bfa20 fffffb8f`5d29a730 ffffd98f`2a7bf060 00000000`00000000 : nt!PnpDeleteLockedDeviceNode+0x52**

**fffffb8f`5d29a6f0 fffff807`464c8c1c     : ffffd98f`2a7bf060 00000000`00000002 ffffd98f`2a7bf060 00000000`00000000 : nt!PnpDeleteLockedDeviceNodes+0xcf**

**fffffb8f`5d29a770 fffff807`464c6255     : fffffb8f`5d29a8b0 ffffd98f`2a7bfa00 ffffd98f`51e25700 ffff9201`00000005 : nt!PnpProcessQueryRemoveAndEject+0x2fc**

**fffffb8f`5d29a850 fffff807`465172e5     : ffff9201`55bd1630 ffff9201`51183b30 ffffd98f`27ab4a00 00000000`00000000 : nt!PnpProcessTargetDeviceEvent+0x109**

**fffffb8f`5d29a880 fffff807`4608faef     : ffffd98f`27ab4aa0 ffffd98f`54397040 ffffd98f`51e25740 fffff807`00000000 : nt!PnpDeviceEventWorker+0x2c5**

**fffffb8f`5d29a900 fffff807`46132815     : ffffd98f`54397040 00000000`00000000 ffffd98f`54397040 00000000`00000000 : nt!ExpWorkerThread+0x14f**

**fffffb8f`5d29aaf0 fffff807`462215f4     : ffffc601`1abc0180 ffffd98f`54397040 fffff807`461327c0 00000000`00000246 : nt!PspSystemThreadStartup+0x55**

**fffffb8f`5d29ab40 00000000`00000000     : fffffb8f`5d29b000 fffffb8f`5d294000 00000000`00000000 00000000`00000000 : nt!KiStartSystemThread+0x34**

**14: kd> .frame /r 4**

**04 fffffb8f`5d2999a0 fffff807`497e52b6     tcpip!FlUnbindAdapter+0x8827a**

**rax=0000000000000000 rbx=ffffd98f4f0307e0 rcx=0000000000000000**

**rdx=0000000000000000 rsi=000000000000000a rdi=fffff80749c1ca70**

**rip=fffff80749b231fa rsp=fffffb8f5d2999a0 rbp=fffffb8f5d299aa0**

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

**r11=0000000000000000 r12=0000000000000000 r13=ffffd98f44c5a100**

**r14=0000000000000000 r15=0000000000000004**

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

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

**tcpip!FlUnbindAdapter+0x8827a:**

**fffff807`49b231fa 90              nop**

**14: kd> dv /V**

**fffffb8f`5d299b20 @rsp+0x0180                UnbindContext = 0xfffffb8f`5d299bf0**

**@rbx              @rbx              ProtocolBindingContext = 0xffffd98f`4f0307e0**

**@esi              @esi                             IfIndex = 0xa**

**@rdi              @rdi                       ProviderState = 0xfffff807`49c1ca70**

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

**14: kd> dt PFL\_INTERFACE  0xffffd98f`4f0307e0 WolOperationsCompleteEvent.Header.SignalState**

**tcpip!PFL\_INTERFACE**

**0xfffff807`49c2b3a0**

**+0x308 WolOperationsCompleteEvent                    :**

**+0x000 Header                                        :**

**+0x004 SignalState                                   : 0n0**

**14: kd> ?  0xffffd98f`4f0307e0+308**

**Evaluate expression: -42265447560472 = ffffd98f`4f030ae8**

<https://hsdes.intel.com/appstore/article/#/14018977791>

(WIFI-294183)[WIN11][SV2][WDI] 0x9F - ndis!ndisPauseFilter:

This is Bugcheck 9F - DRIVER\_POWER\_STATE\_FAILURE (9f) – see attached memory dump:

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

**DRIVER\_POWER\_STATE\_FAILURE (9f)**

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

**Arguments:**

**Arg1: 0000000000000004, The power transition timed out waiting to synchronize with the Pnp**

**subsystem.**

**Arg2: 000000000000012c, Timeout in seconds.**

**Arg3: ffff80095e038040, The thread currently holding on to the Pnp lock.**

**Arg4: fffffd01cdb977e0, nt!TRIAGE\_9F\_PNP on Win7 and higher**

**15: kd> .thread /p /r ffff80095e038040**

**Implicit thread is now ffff8009`5e038040**

…

NativeWiFi Miniport Driver is processing PnP removal IRP:

**15: kd> !thread ffff80095e038040**

**THREAD ffff80095e038040  Cid 0004.39e0  Teb: 0000000000000000 Win32Thread: 0000000000000000 STANDBY**

**IRP List:**

**ffff80095d41bdb0: (0006,01f0) Flags: 00000000  Mdl: 00000000**

**Not impersonating**

**DeviceMap                 ffffa70f79804370**

**Owning Process            ffff8009448ce040       Image:         System**

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

**Wait Start TickCount      781250         Ticks: 2 (0:00:00:00.031)**

**Context Switch Count      101493         IdealProcessor: 15  NoStackSwap**

**UserTime                  00:00:00.000**

**KernelTime                00:00:00.375**

**Win32 Start Address nt!ExpWorkerThread (0xfffff80057818830)**

**Stack Init fffffd01d1537c30 Current fffffd01d1536440**

**Base fffffd01d1538000 Limit fffffd01d1531000 Call 0000000000000000**

**Priority 15 BasePriority 12 PriorityDecrement 48 IoPriority 2 PagePriority 5**

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

**fffffd01`d1536480 fffff800`578cb6c5     : ffff9600`891b4180 00000000`00000000 ffff8009`44982040 ffff9600`891b4180 : nt!KiSwapContext+0x76**

**fffffd01`d15365c0 fffff800`578ccae7     : ffff8009`5e038040 ffff8009`00000000 00000000`00000000 00000000`00000000 : nt!KiSwapThread+0xb05**

**fffffd01`d1536710 fffff800`578cf106     : ffff8009`00000000 004fe07f`00000001 ffff9600`00000000 00000000`00000000 : nt!KiCommitThreadWait+0x137**

**fffffd01`d15367c0 fffff800`5a91febb     : fffffd01`000000fe 00000000`00004e20 fffff800`56d46048 ffff8009`53a1ddd0 : nt!KeWaitForSingleObject+0x256**

**fffffd01`d1536b60 fffff800`56cd094c     : ffff8009`54050010 fffff800`56d46048 ffff8009`53a1ddd0 ffff8009`00000000 : ndis!NdisMSleep+0x7b**

**fffffd01`d1536be0 fffff800`56cd402e     : ffff8009`54050010 00000000`0000ff00 ffff8009`67c40066 fffffd01`d1536c78 : nwifi!MP6Pause+0xdc**

**fffffd01`d1536c10 fffff800`5a9ef3d1     : ffff8009`53fdeb30 fffff800`5a9d3048 ffff8009`53a1ddd0 fffffd01`d1536d28 : nwifi!FilterPause+0x7e**

**fffffd01`d1536c50 fffff800`5aa279c9     : ffff8009`4d3f51a0 fffffd01`d1536cf9 ffff8009`53fdebc0 ffff8009`53fdeb30 : ndis!ndisFInvokePause+0x81**

**fffffd01`d1536ca0 fffff800`5a9ef2ac     : ffffa70f`7c6f8d30 ffffa70f`7c6f8d30 ffffa70f`7c6f8d30 ffffa70f`7c6f8d30 : ndis!ndisPauseFilterInner+0x185**

**fffffd01`d1536d60 fffff800`5a9f26d3     : ffff8009`4d3f6598 fffffd01`d1536ec0 ffffa70f`7c6f8d30 00000000`00000006 : ndis!ndisPauseFilter+0xb8**

**fffffd01`d1536dc0 fffff800`5a9f217f     : ffff8009`4d3f51a0 ffff8009`4d3f51a0 ffff8009`4d3f6610 ffff8009`4d3f6598 : ndis!Ndis::BindEngine::Iterate+0x273**

**fffffd01`d1536f70 fffff800`5a9f53be     : 00000000`00000000 ffff8009`4d3f6598 ffff8009`4d3f6598 fffffd01`d1537100 : ndis!Ndis::BindEngine::UpdateBindings+0xe3**

**fffffd01`d1537020 fffff800`5a9f52e4     : ffff8009`4d3f6598 00000000`00000000 ffff8009`4b03ca01 fffff800`5a9f2dc7 : ndis!Ndis::BindEngine::DispatchPendingWork+0x4a**

**fffffd01`d1537050 fffff800`5aa3284d     : ffff8009`4d3f51a0 fffffd01`d15371a0 ffff8009`4d3f6598 ffff8009`4b03cab0 : ndis!Ndis::BindEngine::ApplyBindChanges+0x54**

**fffffd01`d15370a0 fffff800`5a95f4fb     : ffff8009`4d3f51a0 ffff8009`4d3f51a0 00000000`00000000 fffff800`5a9d3048 : ndis!ndisPnPRemoveDevice+0x2ed**

**fffffd01`d15372e0 fffff800`5aa14d44     : ffff8009`4d3f51a0 ffff8009`4d3f5050 00000000`00000000 ffff8009`5d41bdb0 : ndis!ndisPnPRemoveDeviceEx+0x13f**

**fffffd01`d1537330 fffff800`5a9259c9     : ffff8009`5d41bdb0 fffffd01`d15373e0 ffff8009`4d3f51a0 00000000`00000000 : ndis!ndisPnPIrpRemoveDevice+0x134**

**fffffd01`d15373a0 fffff800`578d00a5     : ffff8009`4d2e9c01 fffffd01`d1537560 00000001`00060001 ffff8009`4d2ea8b0 : ndis!ndisPnPDispatch+0x1b4e9**

**fffffd01`d1537410 fffff800`593984aa     : fffffd01`d1537560 ffff8009`4d2ea8b0 00000000`00000000 ffff8009`4d2ea8b0 : nt!IofCallDriver+0x55**

**(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : Wdf01000!FxIrp::CallDriver+0x16 (Inline Function @ fffff800`593984aa)**

**fffffd01`d1537450 fffff800`5939645a     : 00000000`00000001 00000000`00000001 ffff8009`4d2ea8b0 fffffd01`d1537560 : Wdf01000!FxPkgFdo::ProcessRemoveDeviceOverload+0x8a**

**fffffd01`d1537480 fffff800`59327a93     : ffff8009`4d2ea8b0 00000000`00000000 00000000`00000000 ffff8009`4d2e9c50 : Wdf01000!FxPkgPnp::\_PnpRemoveDevice+0x11a**

**fffffd01`d15374f0 fffff800`59327b40     : ffff8009`5d41bdb0 ffff8009`5d41bdb0 ffff8009`4d2e9c50 00000000`00000000 : Wdf01000!FxPkgPnp::Dispatch+0xd3**

**(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : Wdf01000!DispatchWorker+0x2d (Inline Function @ fffff800`59327b40)**

**(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : Wdf01000!FxDevice::Dispatch+0x3c (Inline Function @ fffff800`59327b40)**

**fffffd01`d1537560 fffff800`578d00a5     : ffff8009`4d2e9c50 fffff800`5792ba30 00000000`00000000 fffffd01`d15376a0 : Wdf01000!FxDevice::DispatchWithLock+0x80**

**fffffd01`d15375b0 fffff800`57d85a24     : ffff8009`4d2e9c50 00000000`00000000 fffffd01`d15376a0 ffff8009`5d41bdb0 : nt!IofCallDriver+0x55**

**fffffd01`d15375f0 fffff800`57d14ddc     : 00000000`00000002 ffff8009`47b8c060 ffff8009`47b8ca20 ffff8009`47b8c060 : nt!IopSynchronousCall+0xf8**

**fffffd01`d1537660 fffff800`578f4274     : ffffa70f`961b7710 ffff8009`47b8ca20 00000000`00000200 00000000`0000000a : nt!IopRemoveDevice+0x108**

**fffffd01`d1537710 fffff800`57d14972     : ffff8009`47b8c060 ffff8009`47b8ca20 00000000`00000000 cb3a4008`00200001 : nt!PnpRemoveLockedDeviceNode+0x1a8**

**fffffd01`d1537770 fffff800`57d146e7     : ffff8009`47b8ca20 fffffd01`d15377f0 ffff8009`47b8c060 00000000`00000000 : nt!PnpDeleteLockedDeviceNode+0x4e**

**fffffd01`d15377b0 fffff800`57d1383c     : ffff8009`47b8c060 00000000`00000002 ffff8009`47b8c060 00000000`00000000 : nt!PnpDeleteLockedDeviceNodes+0xcf**

**fffffd01`d1537830 fffff800`57d8fd7d     : fffffd01`d1537970 ffff8009`47b8ca00 ffff8009`5a478700 ffffa70f`00000004 : nt!PnpProcessQueryRemoveAndEject+0x388**

**fffffd01`d1537910 fffff800`57d03630     : ffffa70f`961b7710 ffffa70f`8b8966c0 ffff8009`4489dc00 00000000`00000000 : nt!PnpProcessTargetDeviceEvent+0x109**

**fffffd01`d1537940 fffff800`57818985     : ffff8009`4489dcf0 ffff8009`5e038040 fffffd01`d1537ac0 fffff800`00000000 : nt!PnpDeviceEventWorker+0x2c0**

**fffffd01`d15379c0 fffff800`5780f5b7     : ffff8009`5e038040 00000000`000003da ffff8009`5e038040 fffff800`57818830 : nt!ExpWorkerThread+0x155**

**fffffd01`d1537bb0 fffff800`57a2e2e4     : ffff9600`89518180 ffff8009`5e038040 fffff800`5780f560 00000000`00000000 : nt!PspSystemThreadStartup+0x57**

**fffffd01`d1537c00 00000000`00000000     : fffffd01`d1538000 fffffd01`d1531000 00000000`00000000 00000000`00000000 : nt!KiStartSystemThread+0x34**

The NativeWiFi Miniport Driver appears to be waiting for its activities to quiesce, but at the same time is blocked in another thread waiting for a mutex:

**15: kd> .thread /p /r ffff80095d751080**

**Implicit thread is now ffff8009`5d751080**

**Process ffff8009`540d5080 has invalid page directories**

**15: kd> kn**

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

**# Child-SP          RetAddr               Call Site**

**00 fffffd01`d3486ec0 fffff800`578cb6c5     nt!KiSwapContext+0x76**

**01 fffffd01`d3487000 fffff800`578ccae7     nt!KiSwapThread+0xb05**

**02 fffffd01`d3487150 fffff800`578cf106     nt!KiCommitThreadWait+0x137**

**03 fffffd01`d3487200 fffff800`56cb6728     nt!KeWaitForSingleObject+0x256**

**04 (Inline Function) --------`--------     nwifi!NwfAcquireMutex+0x2b**

**05 (Inline Function) --------`--------     nwifi!PtAddIoctlReference+0x3b**

**06 fffffd01`d34875a0 fffff800`56cbd4fc     nwifi!IoctlProcessIO+0x58**

**07 fffffd01`d3487610 fffff800`56cbc563     nwifi!IoctlSerializeIO+0xd0**

**08 fffffd01`d3487640 fffff800`5a8e5e9f     nwifi!Dot11DispatchDevCtrl+0x63**

**09 (Inline Function) --------`--------     ndis!ndisDummyHandler+0xdc**

**0a fffffd01`d3487670 fffff800`578d00a5     ndis!ndisDummyIrpHandler+0xff**

**0b fffffd01`d34876c0 fffff800`57cdcfc0     nt!IofCallDriver+0x55**

**0c fffffd01`d3487700 fffff800`57cdb58c     nt!IopSynchronousServiceTail+0x1d0**

**0d fffffd01`d34877b0 fffff800`57cd9866     nt!IopXxxControlFile+0x72c**

**0e fffffd01`d34879c0 fffff800`57a3e0e8     nt!NtDeviceIoControlFile+0x56**

**0f fffffd01`d3487a30 00007fff`8e8aed34     nt!KiSystemServiceCopyEnd+0x28**

**10 00000077`114ff1b8 00000000`00000000     0x00007fff`8e8aed34**

Switching to the frame, the mutex is held by the thread which holds the PnP engine lock:

**15: kd> .frame /r 4**

**04 (Inline Function) --------`--------     nwifi!NwfAcquireMutex+0x2b**

**rax=0000000000000000 rbx=ffff800954050010 rcx=0000000000000000**

**rdx=0000000000000000 rsi=ffff800953fbd2e0 rdi=ffff800954051c30**

**rip=fffff80056cb6728 rsp=fffffd01d34875a0 rbp=0000000000000004**

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

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

**r14=ffff800953fbd3b0 r15=0000000000000001**

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

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

**nwifi!NwfAcquireMutex+0x2b [inlined in nwifi!IoctlProcessIO+0x58]:**

**fffff800`56cb6728 65488b042588010000 mov   rax,qword ptr gs:[188h] gs:00000000`00000188=????????????????**

**15: kd> dt Mutex**

**Local var @ rdi Type \_NWF\_MUTEX\***

**+0x000 Event            : \_KEVENT**

**+0x018 LockOwner        : 0xffff8009`5e038040 \_ETHREAD**

This appears to be a deadlock in the NativeWiFi Miniport Driver (nwifi.sys).

<https://hsdes.intel.com/appstore/article/#/22016967343>

IPS00724451: UUT hung up with black Screen (BSE 0x124) after 36th cycles running S3 WOL.:

The LAN device 8086:1533 (3/0/0) has raised UR AER and this is a fatal error.  
 **0: kd> !analyze -show**

**WHEA\_UNCORRECTABLE\_ERROR (124)**

**A fatal hardware error has occurred. Parameter 1 identifies the type of error**

**source that reported the error. Parameter 2 holds the address of the**

**nt!\_WHEA\_ERROR\_RECORD structure that describes the error condition. Try !errrec Address of the nt!\_WHEA\_ERROR\_RECORD structure to get more details.**

**Arguments:**

**Arg1: 0000000000000004, PCI Express Error**

**Arg2: ffff90873a8e3028, Address of the nt!\_WHEA\_ERROR\_RECORD structure.**

**Arg3: 0000000000000000**

**Arg4: 0000000000000000**

**0: kd> !errrec ffff90873a8e3028**

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

**Common Platform Error Record @ ffff90873a8e3028**

**-------------------------------------------------------------------------------**

**Record Id     : 01d88a52efb3061c**

**Severity      : Fatal (1)**

**Length        : 672**

**Creator       : Microsoft**

**Notify Type   : PCI Express Error**

**Timestamp     : 6/27/2022 19:29:46 (UTC)**

**Flags         : 0x00000000**

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

**Section 0     : PCI Express**

**-------------------------------------------------------------------------------**

**Descriptor    @ ffff90873a8e30a8**

**Section       @ ffff90873a8e3138**

**Offset        : 272**

**Length        : 208**

**Flags         : 0x00000001 Primary**

**Severity      : Recoverable**

**Port Type     : Endpoint**

**Version       : 1.1**

**Command/Status: 0x0500/0x4018**

**Device Id     :**

**VenId:DevId : 8086:1533**

**Class code  : 010000**

**Function No : 0x00**

**Device No   : 0x00**

**Segment     : 0x0000**

**Primary Bus : 0x03**

**Second. Bus : 0x00**

**Slot        : 0x0000**

**Dev. Serial # : 6805caffff882b86**

**Express Capability Information @ ffff90873a8e316c**

**Device Caps : 10008cc2 Role-Based Error Reporting: 1**

**Device Ctl  : 2037 ur FE NF CE**

**Dev Status  : 001a UR fe NF ce**

**Root Ctl   : 0000 fs nfs cs**

**AER Information @ ffff90873a8e31a8**

**Uncorrectable Error Status    : 00100000 UR ecrc mtlp rof uc ca cto fcp ptlp sd dlp und**

**Uncorrectable Error Mask      : 00000000 ur ecrc mtlp rof uc ca cto fcp ptlp sd dlp und**

**Uncorrectable Error Severity  : 00462031 ur ecrc MTLP ROF uc ca cto FCP ptlp SD DLP UND**

**Correctable Error Status      : 00000000 adv rtto rnro dllp tlp re**

**Correctable Error Mask        : 00000000 adv rtto rnro dllp tlp re**

**Caps & Control                : 000000b4 ecrcchken ECRCCHKCAP ecrcgenen ECRCGENCAP FEP**

**Header Log                    : 40000001 0000000f d2201680 d2201680**

**Root Error Command            : 00000007 FEN NFEN CEN**

**Root Error Status             : 00000024 MSG# 00 fer NFER fuf mur UR mcr cer**

**Correctable Error Source ID   : 00,00,00**

**Correctable Error Source ID   : 03,00,00**

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

**Section 1     : Processor Generic**

**-------------------------------------------------------------------------------**

**Descriptor    @ ffff90873a8e30f0**

**Section       @ ffff90873a8e3208**

**Offset        : 480**

**Length        : 192**

**Flags         : 0x00000000**

**Severity      : Informational**

**No valid data fields are present.**

**0: kd> !pcitree**

**Bus 0x0 (FDO Ext ffff908737c968e0)**

**…**

**Bus 0x3 (FDO Ext ffff90873a4ed720)**

**(d=0,  f=0) 80861533 devext 0xffff90873a8f16c0 devstack 0xffff90873a8f1570 0200 Network Controller/Ethernet**

**…**

**0: kd> !pcicfglog 0xffff90873a8f16c0**

**#             Time            CPU   Cid   Tid    F     Offset    Length       Data        Source**

**----  ------------------------  ----  ----  ----  ----  --------  --------  ------------  --------**

**…**

**0056     0x0000000953a30378     0010  0004  14504   Rd    0x0004    0x0002    0x00000506    pci!PciDisableInterrupts+0x2c (fffff804`0c8686c0)**

**0057     0x0000000953a30390     0010  0004  14504   Wr    0x0004    0x0002    0x00000506    pci!PciDisableInterrupts+0x4b (fffff804`0c8686df)**

**0058     0x0000000953a303af     0010  0004  14504   Rd    0x0072    0x0002    0x00008004    pci!PciMaskMsiXInterrupt+0x3a (fffff804`0c86f5ee)**

**0059     0x0000000953a303d9     0010  0004  14504   Wr    0x0072    0x0002    0x00000004    pci!PciMaskMsiXInterrupt+0x60 (fffff804`0c86f614)**

**0060     0x0000000953a30401     0010  0004  14504   Rd    0x0052    0x0002    0x00000180    pci!PciMaskMsiInterrupt+0x2f (fffff804`0c8636b7)**

**0061     0x0000000953a30429     0010  0004  14504   Wr    0x0052    0x0002    0x00000180    pci!PciMaskMsiInterrupt+0x55 (fffff804`0c8636dd)**

**0062     0x0000000953a30444     0010  0004  14504   Rd    0x0004    0x0002    0x00000506    pci!PciDisconnectDevice+0x74 (fffff804`0c863760)**

**0063     0x0000000953a3046b     0010  0004  14504   Wr    0x0004    0x0002    0x00000500    pci!PciDisconnectDevice+0xc6 (fffff804`0c8637b2)**

**0064     0x0000000953a3049c     0010  0004  14504   Rd    0x00aa    0x0002    0x00000010    pci!ExpressCheckForPendingTransactions+0x26 (fffff804`0c881e72)**

**0065     0x0000000953a304bc     0010  0004  14504   Rd    0x0040    0x0008    0xc8235001    pci!PciSetHardwarePowerStatePreamble+0x32 (fffff804`0c867e32)**

**0066     0x0000000953a304e5     0010  0004  14504   Wr    0x0044    0x0002    0x0000210b    pci!PciSetHardwarePowerStateDispatch+0x21a (fffff804`0c868c7e)**

**0067     0x0000000953a3249b     0000  13140  1140   Rd    0x0100    0x002c    0x14020001    pci!PciRpRcecHandleAerInterrupt+0x220 (fffff804`0c88cd30)**

**0068     0x0000000953a32a1c     0000  13140  1140   Rd    0x0004    0x0002    0x00000500    pci!PciInitWheaErrorPacket+0xba (fffff804`0c88c9a2)**

**0069     0x0000000953a32b0e     0000  13140  1140   Rd    0x0006    0x0002    0x00004018    pci!PciInitWheaErrorPacket+0xcf (fffff804`0c88c9b7)**

**0070     0x0000000953a32b94     0000  13140  1140   Rd    0x00a0    0x0014    0x00020010    pci!PciInitWheaErrorPacket+0x1c2 (fffff804`0c88caaa)**

**0071     0x0000000953a32f7e     0000  13140  1140   Wr    0x0104    0x0004    0xffffffff    pci!PciClearAerStatus+0x5c (fffff804`0c872fe0)**

**0072     0x0000000953a32ff6     0000  13140  1140   Wr    0x0110    0x0004    0xffffffff    pci!PciClearAerStatus+0x86 (fffff804`0c87300a)**

<https://hsdes.intel.com/appstore/article/#/22016758886>

BSOD observed during teams call sue to AV\_pacer!PcpMrkComputeMarking [pacer.sys]

QoS Packet Scheduler (PACER.SYS) is trying to acquire a spinlock, but the spinlock is located in already freed pool block:

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

**IRQL\_NOT\_LESS\_OR\_EQUAL (a)**

**An attempt was made to access a pageable (or completely invalid) address at an**

**interrupt request level (IRQL) that is too high.  This is usually**

**caused by drivers using improper addresses.**

**If a kernel debugger is available get the stack backtrace.**

**Arguments:**

**Arg1: 0000000000000018, memory referenced**

**Arg2: 0000000000000002, IRQL**

**Arg3: 0000000000000001, bitfield :**

**bit 0 : value 0 = read operation, 1 = write operation**

**bit 3 : value 0 = not an execute operation, 1 = execute operation (only on chips which support this level of status)**

**Arg4: fffff80180cc7f7c, address which referenced memory**

**8: kd> u fffff80180cc7f7c L1**

**nt!KxWaitForLockOwnerShip+0x4c:**

**fffff801`80cc7f7c 48890a          mov     qword ptr [rdx],rcx**

**8: kd> r cr2**

**cr2=0000000000000018**

**8: kd> k**

**# Child-SP          RetAddr               Call Site**

**00 fffffe01`0852e1f8 fffff801`80e3e9a9     nt!KeBugCheckEx**

**01 fffffe01`0852e200 fffff801`80e3a034     nt!KiBugCheckDispatch+0x69**

**02 fffffe01`0852e340 fffff801`80cc7f7c     nt!KiPageFault+0x474**

**03 fffffe01`0852e4d0 fffff801`80c9b65c     nt!KxWaitForLockOwnerShip+0x4c**

**04 fffffe01`0852e530 fffff801`9c6fc4a4     nt!KeAcquireInStackQueuedSpinLock+0xac**

**05 (Inline Function) --------`--------     pacer!RtlAcquireWriteLock+0x33**

**06 fffffe01`0852e560 fffff801`9c6f9f93     pacer!PcpMrkComputeMarking+0x5c**

**07 fffffe01`0852e5d0 fffff801`82f10afe     pacer!PcQoSPQueryTrafficClass+0x73**

**08 fffffe01`0852e610 fffff801`830a8b92     NETIO!NetioQueryNetBufferListTrafficClass+0x4e**

**09 fffffe01`0852e650 fffff801`830c8154     tcpip!IppSendDatagramsCommon+0x4f2**

**0a fffffe01`0852e810 fffff801`830c6a3a     tcpip!UdpSendMessagesOnPath+0x1194**

**0b fffffe01`0852ec40 fffff801`830c6745     tcpip!UdpSendMessages+0x2da**

**0c fffffe01`0852f000 fffff801`80cd406a     tcpip!UdpTlProviderSendMessagesCalloutRoutine+0x15**

**0d fffffe01`0852f030 fffff801`80cd3fdd     nt!KeExpandKernelStackAndCalloutInternal+0x7a**

**0e fffffe01`0852f0a0 fffff801`830f2f0a     nt!KeExpandKernelStackAndCalloutEx+0x1d**

**0f fffffe01`0852f0e0 fffff801`9c4879a9     tcpip!UdpTlProviderSendMessages+0x7a**

**10 fffffe01`0852f150 fffff801`9c48722d     afd!AfdFastDatagramSend+0x709**

**11 fffffe01`0852f390 fffff801`810db2ce     afd!AfdFastIoDeviceControl+0x184d**

**12 fffffe01`0852f730 fffff801`810d9866     nt!IopXxxControlFile+0x46e**

**13 fffffe01`0852f940 fffff801`80e3e0e5     nt!NtDeviceIoControlFile+0x56**

**14 fffffe01`0852f9b0 00007ff9`25b0ed34     nt!KiSystemServiceCopyEnd+0x25**

**15 000000da`a57fea48 00000000`00000000     0x00007ff9`25b0ed34**

**8: kd> .frame /r 4**

**04 fffffe01`0852e530 fffff801`9c6fc4a4     nt!KeAcquireInStackQueuedSpinLock+0xac**

**rax=0000000000000000 rbx=0000000000000002 rcx=fffffe010852e590**

**rdx=0000000000000018 rsi=ffffa28955ce9920 rdi=ffffa28955ce9920**

**rip=fffff80180c9b65c rsp=fffffe010852e530 rbp=ffffa2895a45f3f0**

**r8=0000000000000001  r9=fffffe010852e63c r10=ffffa28955ce9980**

**r11=fffffe010852e5c8 r12=fffff801832969d0 r13=0000000000000125**

**r14=fffffe010852e63c r15=ffffa2892a11aa78**

**iopl=0         nv up ei ng nz na po nc**

**cs=0010  ss=0018  ds=002b  es=002b  fs=0053  gs=002b             efl=00040286**

**nt!KeAcquireInStackQueuedSpinLock+0xac:**

**fffff801`80c9b65c 4883c428        add     rsp,28h**

**8: kd> ub**

**nt!KeAcquireInStackQueuedSpinLock+0x97:**

**fffff801`80c9b647 c3              ret**

**fffff801`80c9b648 cc              int     3**

**fffff801`80c9b649 498bd0          mov     rdx,r8**

**fffff801`80c9b64c 498712          xchg    rdx,qword ptr [r10]**

**fffff801`80c9b64f 4885d2          test    rdx,rdx**

**fffff801`80c9b652 7408            je      nt!KeAcquireInStackQueuedSpinLock+0xac (fffff801`80c9b65c)**

**fffff801`80c9b654 498bc8          mov     rcx,r8**

**fffff801`80c9b657 e8d4c80200      call    nt!KxWaitForLockOwnerShip (fffff801`80cc7f30)**

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

**05 (Inline Function) --------`--------     pacer!RtlAcquireWriteLock+0x33**

**rax=0000000000000000 rbx=0000000000000002 rcx=fffffe010852e590**

**rdx=0000000000000018 rsi=ffffa28955ce9920 rdi=ffffa28955ce9920**

**rip=fffff8019c6fc4a4 rsp=fffffe010852e560 rbp=ffffa2895a45f3f0**

**r8=0000000000000001  r9=fffffe010852e63c r10=ffffa28955ce9980**

**r11=fffffe010852e5c8 r12=fffff801832969d0 r13=0000000000000125**

**r14=fffffe010852e63c r15=ffffa2892a11aa78**

**iopl=0         nv up ei ng nz na po nc**

**cs=0010  ss=0018  ds=002b  es=002b  fs=0053  gs=002b             efl=00040286**

**pacer!RtlAcquireWriteLock+0x33 [inlined in pacer!PcpMrkComputeMarking+0x5c]:**

**fffff801`9c6fc4a4 8b4668          mov     eax,dword ptr [rsi+68h] ds:002b:ffffa289`55ce9988=00000010**

**8: kd> ub**

**pacer!PcpMrkComputeMarking+0x39:**

**fffff801`9c6fc481 6683e001        and     ax,1**

**fffff801`9c6fc485 0fb7d8          movzx   ebx,ax**

**fffff801`9c6fc488 6683cb02        or      bx,2**

**fffff801`9c6fc48c 4183f809        cmp     r8d,9**

**fffff801`9c6fc490 660f45d8        cmovne  bx,ax**

**fffff801`9c6fc494 4883c160        add     rcx,60h**

**fffff801`9c6fc498 4c8b1549a00000  mov     r10,qword ptr [pacer!\_imp\_KeAcquireInStackQueuedSpinLock (fffff801`9c7064e8)]**

**fffff801`9c6fc49f e80cf159e4      call    nt!KeAcquireInStackQueuedSpinLock (fffff801`80c9b5b0)**

**8: kd> ub fffff801`9c6fc481**

**pacer!PcpMrkComputeMarking+0x1d:**

**fffff801`9c6fc465 488bea          mov     rbp,rdx**

**fffff801`9c6fc468 0f11442430      movups  xmmword ptr [rsp+30h],xmm0**

**fffff801`9c6fc46d 498943d8        mov     qword ptr [r11-28h],rax**

**fffff801`9c6fc471 498d53c8        lea     rdx,[r11-38h]**

**fffff801`9c6fc475 8b4130          mov     eax,dword ptr [rcx+30h]**

**fffff801`9c6fc478 488bf1          mov     rsi,rcx**

**fffff801`9c6fc47b c1e80e          shr     eax,0Eh**

**fffff801`9c6fc47e 4d8bf1          mov     r14,r9**

**8: kd> !pool ffffa28955ce9920+60**

**Pool page ffffa28955ce9980 region is Nonpaged pool**

**ffffa28955ce9000 size:  900 previous size:    0  (Allocated)  @GM6**

**\*ffffa28955ce9900 size:  3c0 previous size:    0  (Free)      \*nz.,**

**Owning component : Unknown (update pooltag.txt)**

**ffffa28955ce9cd0 size:  250 previous size:    0  (Allocated)  ALPC**

**ffffa28955ce9f20 size:   c0 previous size:    0  (Free)       .z.,**

<https://hsdes.intel.com/appstore/article/#/22016708823>

[HLK][MTL-H][RVP][BSP] System - Sleep with IO Before and After (Reliability Sysfund) Causing BSOD:

This is a memory leak in ibtusb.sys:

**0: 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: ffffe408683dc820, name of the driver having the issue.**

**Arg3: ffffe4084c8fd9d0, verifier internal structure with driver information.**

**Arg4: 0000000000000001, 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.**

**0: kd> du ffffe408683dc820**

**ffffe408`683dc820  "ibtusb.sys"**

**0: kd> !verifier 3 ibtusb.sys**

**Verify Flags Level 0x00120b19**

**…**

**Pool Allocations:**

**Address             Length      Tag   Caller Address**

**------------------  ----------  ----  ------------------**

**0xffffe40878ceafa0  0x0000005a  0VWF  0xfffff8000d288ecd  ibtusb!ExAllocatePoolZero+0x2d**

<https://hsdes.intel.com/appstore/article/#/16019742609>

[CSPV][CSPV\_SH][DELL][ADL][WOS][BSOD] - AV\_BthA2dp!SidebandAudioWdmEndpoint::SignalStatusUpdate:

BthA2dp!SidebandAudioWdmEndpoint::SignalStatusUpdate attempts to dereference a NULL pointer because it does not check if status update queue is empty:

**11: 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: fffff8010f71814e, The address that the exception occurred at**

**Arg3: ffff9985a2a9f498, Exception Record Address**

**Arg4: ffff9985a2a9ecb0, Context Record Address**

**11: kd> u fffff8010f71814e L1**

**BthA2dp!CompletableIrp::{ctor}+0xa [inlined in BthA2dp!SidebandAudioWdmEndpoint::SignalStatusUpdate+0x18e]:**

**fffff801`0f71814e 488b5038        mov     rdx,qword ptr [rax+38h]**

**11: kd> r cr2**

**cr2=0000000000000038**

**11: kd> k**

**# Child-SP          RetAddr               Call Site**

**00 ffff9985`a2a9e428 fffff801`19247787     nt!KeBugCheckEx**

**01 ffff9985`a2a9e430 fffff801`191eb121     nt!PspSystemThreadStartup$filt$0+0x44**

**02 ffff9985`a2a9e470 fffff801`1923418f     nt!\_C\_specific\_handler+0xa1**

**03 ffff9985`a2a9e4e0 fffff801`1900fac3     nt!RtlpExecuteHandlerForException+0xf**

**04 ffff9985`a2a9e510 fffff801`19013937     nt!RtlDispatchException+0x2f3**

**05 ffff9985`a2a9ec80 fffff801`1923e6fc     nt!KiDispatchException+0x317**

**06 ffff9985`a2a9f360 fffff801`19239c0e     nt!KiExceptionDispatch+0x13c**

**07 ffff9985`a2a9f540 fffff801`0f71814e     nt!KiPageFault+0x44e**

**08 (Inline Function) --------`--------     BthA2dp!CompletableIrp::{ctor}+0xa**

**09 ffff9985`a2a9f6d0 fffff801`0f708008     BthA2dp!SidebandAudioWdmEndpoint::SignalStatusUpdate+0x18e**

**0a ffff9985`a2a9f770 fffff801`0f6ba46a     BthA2dp!A2dpRole::SignalStatusUpdateToSidebandDevice+0xc8**

**0b ffff9985`a2a9f7e0 fffff801`0f6ba798     BthA2dp!A2dpRole::SetConnectionProperties+0x18a**

**0c ffff9985`a2a9f8a0 fffff801`190f221e     BthA2dp!A2dpRole::SetConnectionPropertiesWorker+0x18**

**0d ffff9985`a2a9f8d0 fffff801`190188a5     nt!IopProcessWorkItem+0x8e**

**0e ffff9985`a2a9f940 fffff801`1900f4a7     nt!ExpWorkerThread+0x155**

**0f ffff9985`a2a9fb30 fffff801`1922de84     nt!PspSystemThreadStartup+0x57**

**10 ffff9985`a2a9fb80 00000000`00000000     nt!KiStartSystemThread+0x34**

**11: kd> .frame /r 9**

**09 ffff9985`a2a9f6d0 fffff801`0f708008     BthA2dp!SidebandAudioWdmEndpoint::SignalStatusUpdate+0x18e**

**rax=0000000000000000 rbx=0000000000000000 rcx=ffff878203fe2060**

**rdx=0000000000000000 rsi=ffff878203fe2070 rdi=0000000000000001**

**rip=fffff8010f71814e rsp=ffff9985a2a9f6d0 rbp=ffff878203fe2060**

**r8=0000000000000000  r9=ffff878203fe20d8 r10=fffff801190c8d30**

**r11=ffff878203fe2000 r12=fffff8010f6fe000 r13=fffff8010f6fe058**

**r14=0000000000000000 r15=0000000000000000**

**iopl=0         nv up ei ng nz na po nc**

**cs=0010  ss=0018  ds=002b  es=002b  fs=0053  gs=002b             efl=00040286**

**BthA2dp!SidebandAudioWdmEndpoint::SignalStatusUpdate+0x18e:**

**fffff801`0f71814e 488b5038        mov     rdx,qword ptr [rax+38h] ds:002b:00000000`00000038=????????????????**

**11: kd> dt this m\_statusUpdateQueues[0].IrpList.LockedList.**

**Local var @ rsi Type SidebandAudioWdmEndpoint\***

**+0x078 m\_statusUpdateQueues                        : [0]**

**+0x000 IrpList                                     :**

**+0x000 LockedList                                  :**

**+0x000 ListHead                                    : \_LIST\_ENTRY [ 0xffff8782`03fe20d8 - 0xffff8782`03fe20d8 ]**

**+0x010 SpinLock                                    : 0**

**+0x018 ListLock                                    : 0xffff8782`03fe20e8  -> 0**

**+0x020 Count                                       : 0n0**

<https://hsdes.intel.com/appstore/article/#/22016608086>

[MTLH][RVP][SV3][CS][Cycling] Access Violation Error during 5 CS Cycle Test ( km:access\_violation\_vrf\_unloaded\_ip\_threatintelligence.dll!unknown\_function):

WTD Sensor unloads while having its WNF subscription outstanding:

**3: kd> !analyze -v**

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

**\*                                                                             \***

**\*                        Bugcheck Analysis                                    \***

**\*                                                                             \***

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

**…**

**PROCESS\_NAME:  svchost.exe**

**ERROR\_CODE: (NTSTATUS) 0x80000003 - {EXCEPTION}  Breakpoint  A breakpoint has been reached.**

**EXCEPTION\_CODE\_STR:  80000003**

**EXCEPTION\_PARAMETER1:  0000000000000000**

**CONTEXT:  00000072ad3fee40 -- (.cxr 0x72ad3fee40)**

**rax=0000000000000000 rbx=00007ff9aecde100 rcx=00007ff9dee907b4**

**rdx=0000000000000000 rsi=0000000000000001 rdi=00007ff9aecde0d8**

**rip=00007ff9aec95efb rsp=00000072ad3ff570 rbp=00000072ad3ff600**

**r8=00000072ad3ff508  r9=0000000000000000 r10=0000000000000000**

**r11=0000000000000246 r12=0000000000000000 r13=00007ff9aecde088**

**r14=00007ff9aecbf460 r15=000002667729b940**

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

**cs=0033  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00010206**

**<Unloaded\_ThreatIntelligence.DLL>+0x15efb:**

**00007ff9`aec95efb ??              ???**

**Resetting default scope**

**EXECUTE\_ADDRESS: 7ff9aec95efb**

**FAILED\_INSTRUCTION\_ADDRESS:**

**ThreatIntelligence.DLL+15efb**

**00007ff9`aec95efb ??              ???**

**EXCEPTION\_RECORD:  00000072ad3ff330 -- (.exr 0x72ad3ff330)**

**ExceptionAddress: 00007ff9aec95efb (<Unloaded\_ThreatIntelligence.DLL>+0x0000000000015efb)**

**ExceptionCode: c0000005 (Access violation)**

**ExceptionFlags: 00000000**

**NumberParameters: 2**

**Parameter[0]: 0000000000000008**

**Parameter[1]: 00007ff9aec95efb**

**Attempt to execute non-executable address 00007ff9aec95efb**

**IP\_MODULE\_UNLOADED:**

**ThreatIntelligence.DLL+15efb**

**00007ff9`aec95efb ??              ???**

**STACK\_TEXT:**

**00000072`ad3ff570 00007ff9`ad0b465c     : 00007ff9`aecde100 0000ab39`dcbe7602 00000000`00000008 00000000`0000026c : <Unloaded\_ThreatIntelligence.DLL>+0x15efb**

**00000072`ad3ff578 00007ff9`aecde100     : 0000ab39`dcbe7602 00000000`00000008 00000000`0000026c 0000d015`00001c38 : <Unloaded\_WTDSENSOR.dll>+0x465c**

**00000072`ad3ff580 0000ab39`dcbe7602     : 00000000`00000008 00000000`0000026c 0000d015`00001c38 00007ff9`aecde088 : <Unloaded\_ThreatIntelligence.DLL>+0x5e100**

**00000072`ad3ff588 00000000`00000008     : 00000000`0000026c 0000d015`00001c38 00007ff9`aecde088 00007ff9`aecbf67e : 0x0000ab39`dcbe7602**

**00000072`ad3ff590 00000000`0000026c     : 0000d015`00001c38 00007ff9`aecde088 00007ff9`aecbf67e 00000072`ad3ff649 : 0x8**

**00000072`ad3ff598 0000d015`00001c38     : 00007ff9`aecde088 00007ff9`aecbf67e 00000072`ad3ff649 00007ff9`aecde088 : 0x26c**

**00000072`ad3ff5a0 00007ff9`aecde088     : 00007ff9`aecbf67e 00000072`ad3ff649 00007ff9`aecde088 00000000`00000001 : 0x0000d015`00001c38**

**00000072`ad3ff5a8 00007ff9`aecbf67e     : 00000072`ad3ff649 00007ff9`aecde088 00000000`00000001 00007ff9`aecde0d8 : <Unloaded\_ThreatIntelligence.DLL>+0x5e088**

**00000072`ad3ff5b0 00000072`ad3ff649     : 00007ff9`aecde088 00000000`00000001 00007ff9`aecde0d8 00000266`77130000 : <Unloaded\_ThreatIntelligence.DLL>+0x3f67e**

**00000072`ad3ff5b8 00007ff9`aecde088     : 00000000`00000001 00007ff9`aecde0d8 00000266`77130000 00007ff9`00001030 : 0x00000072`ad3ff649**

**00000072`ad3ff5c0 00000000`00000001     : 00007ff9`aecde0d8 00000266`77130000 00007ff9`00001030 00007ff9`aecde088 : <Unloaded\_ThreatIntelligence.DLL>+0x5e088**

**00000072`ad3ff5c8 00007ff9`aecde0d8     : 00000266`77130000 00007ff9`00001030 00007ff9`aecde088 00000072`ad3ff6e0 : 0x1**

**00000072`ad3ff5d0 00000266`77130000     : 00007ff9`00001030 00007ff9`aecde088 00000072`ad3ff6e0 00000266`77239298 : <Unloaded\_ThreatIntelligence.DLL>+0x5e0d8**

**00000072`ad3ff5d8 00007ff9`00001030     : 00007ff9`aecde088 00000072`ad3ff6e0 00000266`77239298 0000d015`4ebee69a : 0x00000266`77130000**

**00000072`ad3ff5e0 00007ff9`aecde088     : 00000072`ad3ff6e0 00000266`77239298 0000d015`4ebee69a 00000266`77239290 : 0x00007ff9`00001030**

**00000072`ad3ff5e8 00000072`ad3ff6e0     : 00000266`77239298 0000d015`4ebee69a 00000266`77239290 00007ff9`dedf8ca8 : <Unloaded\_ThreatIntelligence.DLL>+0x5e088**

**00000072`ad3ff5f0 00000266`77239298     : 0000d015`4ebee69a 00000266`77239290 00007ff9`dedf8ca8 41821a3a`a3bc0875 : 0x00000072`ad3ff6e0**

**00000072`ad3ff5f8 0000d015`4ebee69a     : 00000266`77239290 00007ff9`dedf8ca8 41821a3a`a3bc0875 00000266`77239170 : 0x00000266`77239298**

**00000072`ad3ff600 00000266`77239290     : 00007ff9`dedf8ca8 41821a3a`a3bc0875 00000266`77239170 00000072`00000000 : 0x0000d015`4ebee69a**

**00000072`ad3ff608 00007ff9`dedf8ca8     : 41821a3a`a3bc0875 00000266`77239170 00000072`00000000 00000000`ad3ff658 : 0x00000266`77239290**

**00000072`ad3ff610 00007ff9`dedf897a     : 00000000`00000000 00000266`77239250 00000000`00000000 00000000`00000000 : ntdll!RtlpWnfWalkUserSubscriptionList+0x254**

**00000072`ad3ff6f0 00007ff9`dedf87d4     : 00000266`7729b940 00000000`00000000 00000000`00000000 00000000`00000000 : ntdll!RtlpWnfProcessCurrentDescriptor+0x10a**

**00000072`ad3ff740 00007ff9`dedfd23e     : 00000266`77206b30 00000266`77206cb8 00000000`7ffe0386 00007ff9`dedfd14c : ntdll!RtlpWnfNotificationThread+0x84**

**00000072`ad3ff7b0 00007ff9`dee0e865     : 00000266`7723d9a0 00000266`77244980 00000000`00000000 00000266`7723d9a0 : ntdll!TppExecuteWaitCallback+0xae**

**00000072`ad3ff800 00007ff9`de9b163d     : 00000050`00000020 00000000`00000000 00000000`00000000 00000000`00000000 : ntdll!TppWorkerThread+0x445**

**00000072`ad3ffab0 00007ff9`dee3d878     : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : KERNEL32!BaseThreadInitThunk+0x1d**

**00000072`ad3ffae0 00000000`00000000     : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : ntdll!RtlUserThreadStart+0x28**

**…**

From another process, where WTD Sensor is still loaded, we can see its version:

**3: kd> .process /p /r ffffe782`79655080**

**Implicit process is now ffffe782`79655080**

**Loading User Symbols**

**................................................................**

**..........................**

**3: kd> lmvi mWTDSENSOR**

**Browse full module list**

**start             end                 module name**

**00007ff9`ad0b0000 00007ff9`ad0ba000   WTDSENSOR   (deferred)**

**Symbol file: WTDSENSOR.dll**

**Image path: C:\windows\system32\WTDSENSOR.dll**

**Image name: WTDSENSOR.dll**

**Browse all global symbols  functions  data**

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

**Timestamp:        AE469780 (This is a reproducible build file hash, not a timestamp)**

**CheckSum:         0000C9D5**

**ImageSize:        0000A000**

**File version:     10.0.25290.1000**

**Product version:  10.0.25290.1000**

**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:     wtdsensor.dll**

**OriginalFilename: wtdsensor.dll**

**ProductVersion:   10.0.25290.1000**

**FileVersion:      10.0.25290.1000 (WinBuild.160101.0800)**

**FileDescription:  WTD Framework Sensor Client**

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

<https://hsdes.intel.com/appstore/article/#/22016589849>

[Win11 OS][SV3][NetCx][WWAN] SYSTEM\_THREAD\_EXCEPTION\_NOT\_HANDLED (7e) in MbbCx.sys after restart:

ndis!ndisVerifierNdisMIndicateStatusEx is dereferencing NULL pointer because ndis!ndisVerifierNdisDispatch is not initialized, which happens because nt!ViFnXdvQueryDispatchTable is not initialized either.

**2: 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: fffff8023cad1fc9, The address that the exception occurred at**

**Arg3: ffffd488fe717228, Exception Record Address**

**Arg4: ffffd488fe716a40, Context Record Address**

**2: kd> !error c0000005**

**Error code: (NTSTATUS) 0xc0000005 (3221225477) - The instruction at 0x%p referenced memory at 0x%p. The memory could not be %s.**

**2: kd> u fffff8023cad1fc9 L1**

**ndis!ndisVerifierNdisMIndicateStatusEx+0x19:**

**fffff802`3cad1fc9 488b4028        mov     rax,qword ptr [rax+28h]**

**2: kd> k**

**# Child-SP          RetAddr               Call Site**

**00 ffffd488`fe7161c8 fffff802`3acb94a2     nt!KeBugCheckEx**

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

**02 ffffd488`fe7161d0 fffff802`3ac4cff1     nt!PspSystemThreadStartup$filt$0+0x44**

**03 ffffd488`fe716210 fffff802`3aca3dcf     nt!\_\_C\_specific\_handler+0xa1**

**04 ffffd488`fe716280 fffff802`3ab296b2     nt!RtlpExecuteHandlerForException+0xf**

**05 ffffd488`fe7162b0 fffff802`3ab2888e     nt!RtlDispatchException+0x2d2**

**06 ffffd488`fe716a10 fffff802`3acae585     nt!KiDispatchException+0x1ae**

**07 ffffd488`fe7170f0 fffff802`3aca989f     nt!KiExceptionDispatch+0x145**

**08 ffffd488`fe7172d0 fffff802`3cad1fc9     nt!KiPageFault+0x45f**

**09 ffffd488`fe717460 fffff80a`6ff379fe     ndis!ndisVerifierNdisMIndicateStatusEx+0x19**

**0a ffffd488`fe7174a0 fffff80a`6ff1d60e     MbbCx!MbbUtilNdisMiniportIndicateStatusEx+0x86**

**0b (Inline Function) --------`--------     MbbCx!MbbNdisMiniportIndicateRequestStatus+0x4e**

**0c ffffd488`fe717520 fffff80a`6ff1d77b     MbbCx!MbbNdisDeviceServiceEventStatusHandler+0x216**

**0d ffffd488`fe717630 fffff80a`6ff311a1     MbbCx!MbbNdisDeviceServiceStatusHandler+0xab**

**0e ffffd488`fe717680 fffff80a`6ff10a5c     MbbCx!MbbUtilCommonCIDResponse+0xa5**

**0f ffffd488`fe7177e0 fffff80a`6ff2de98     MbbCx!MbbNdisIndicateStatus+0xbc**

**10 ffffd488`fe717840 fffff80a`6ff2d0a2     MbbCx!MbbReqFsmResponseReceived+0x68**

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

**12 ffffd488`fe717880 fffff80a`6ff10feb     MbbCx!MbbReqMgrQueueEvent+0x18e**

**13 ffffd488`fe7178f0 fffff80a`6ff113c9     MbbCx!MbbNdisParseStatusIndication+0xef**

**14 ffffd488`fe717950 fffff80a`6ff2ddad     MbbCx!MbbNdisParseResponseFragment+0x169**

**15 ffffd488`fe7179d0 fffff80a`6ff2d0a2     MbbCx!MbbReqFsmSendComplete+0x5d**

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

**17 ffffd488`fe717a00 fffff80a`6ff2cdc5     MbbCx!MbbReqMgrQueueEvent+0x18e**

**18 ffffd488`fe717a70 fffff80a`6ff30190     MbbCx!MbxMessagesHandler+0xb5**

**19 ffffd488`fe717ac0 fffff802`3ab27657     MbbCx!MbbWorkMgrProcessWorkItem+0x120**

**1a ffffd488`fe717b30 fffff802`3ac9b494     nt!PspSystemThreadStartup+0x57**

**1b ffffd488`fe717b80 00000000`00000000     nt!KiStartSystemThread+0x34**

**2: kd> u ndis!ndisVerifierNdisMIndicateStatusEx ndis!ndisVerifierNdisMIndicateStatusEx+0x19**

**ndis!ndisVerifierNdisMIndicateStatusEx:**

**fffff802`3cad1fb0 4883ec38        sub     rsp,38h**

**fffff802`3cad1fb4 488b05bd450400  mov     rax,qword ptr [ndis!ndisVerifierNdisDispatch (fffff802`3cb16578)]**

**fffff802`3cad1fbb 4c8d0d2e90f6ff  lea     r9,[ndis!NdisMIndicateStatusEx (fffff802`3ca3aff0)]**

**fffff802`3cad1fc2 4c8b8160130000  mov     r8,qword ptr [rcx+1360h]**

**fffff802`3cad1fc9 488b4028        mov     rax,qword ptr [rax+28h]**

**2: kd> dq ndis!ndisVerifierNdisDispatch  L1**

**fffff802`3cb16578  00000000`00000000**

**2: kd> dq nt!ViFnXdvQueryDispatchTable L1**

**fffff802`3b5d9a18  00000000`00000000**

<https://hsdes.intel.com/appstore/article/#/13010561873>

[MTL-P][A6][GC][CORP][DPMO]:“Observed Soft hung in OS on SYSTEM\_THREAD\_EXCEPTION\_NOT\_HANDLED bugcheck(7e) pointing to NetAdapterCx.sys module during S4 cycling”:

As the device is leaving D0, NetAdapterCx!ExecutionContext::~ExecutionContext asserts when m\_workerThreadRequested event is signaled.

But management of NetAdapterCx’s worker threads is internal to NetAdapterCx and this asserts leads to Bugcheck SYSTEM\_THREAD\_EXCEPTION\_NOT\_HANDLED (7e).

**11: 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: ffffffffc0000420, The exception code that was not handled**

**Arg2: fffff800660a70f9, The address that the exception occurred at**

**Arg3: fffff2855f9a6ac8, Exception Record Address**

**Arg4: fffff2855f9a62e0, Context Record Address**

**11: kd> !error c0000420**

**Error code: (NTSTATUS) 0xc0000420 (3221226528) - An assertion failure has occurred.**

**11: kd> u fffff800660a70f9 L1**

**NetAdapterCx!ExecutionContext::~ExecutionContext+0x4d:**

**fffff800`660a70f9 cd2c            int     2Ch**

**11: kd> kn**

**# Child-SP          RetAddr               Call Site**

**00 fffff285`5f9a5a58 fffff800`2d847787     nt!KeBugCheckEx**

**01 fffff285`5f9a5a60 fffff800`2d7eb121     nt!PspSystemThreadStartup$filt$0+0x44**

**02 fffff285`5f9a5aa0 fffff800`2d83418f     nt!\_C\_specific\_handler+0xa1**

**03 fffff285`5f9a5b10 fffff800`2d60fac3     nt!RtlpExecuteHandlerForException+0xf**

**04 fffff285`5f9a5b40 fffff800`2d613937     nt!RtlDispatchException+0x2f3**

**05 fffff285`5f9a62b0 fffff800`2d83e6fc     nt!KiDispatchException+0x317**

**06 fffff285`5f9a6990 fffff800`2d83cc7f     nt!KiExceptionDispatch+0x13c**

**07 fffff285`5f9a6b70 fffff800`660a70f9     nt!KiRaiseAssertion+0x33f**

**08 fffff285`5f9a6d00 fffff800`660874b4     NetAdapterCx!ExecutionContext::~ExecutionContext+0x4d**

**09 fffff285`5f9a6d30 fffff800`6606ea34     NetAdapterCx!ExecutionContext::`scalar deleting destructor'+0x14**

**0a (Inline Function) --------`--------     NetAdapterCx!wistd::default\_delete<ExecutionContext>::operator()+0x11**

**0b (Inline Function) --------`--------     NetAdapterCx!wistd::unique\_ptr<ExecutionContext,wistd::default\_delete<ExecutionContext> >::reset+0x25**

**0c (Inline Function) --------`--------     NetAdapterCx!wistd::unique\_ptr<ExecutionContext,wistd::default\_delete<ExecutionContext> >::{dtor}+0x25**

**0d (Inline Function) --------`--------     NetAdapterCx!NxQueue::{dtor}+0x25**

**0e fffff285`5f9a6d60 fffff800`6606e82d     NetAdapterCx!NxQueue::`scalar deleting destructor'+0x34**

**0f (Inline Function) --------`--------     NetAdapterCx!PacketQueueCreate::\_\_l2::<lambda\_aa8db7871828dc0a28edcdc8caf2cfa8>::operator()+0x39**

**10 fffff285`5f9a6d90 fffff800`305144c2     NetAdapterCx!<lambda\_aa8db7871828dc0a28edcdc8caf2cfa8>::<lambda\_invoker\_cdecl>+0x3d**

**11 fffff285`5f9a6dc0 fffff800`30506459     Wdf01000!FxObject::ProcessDestroy+0xf122**

**12 (Inline Function) --------`--------     Wdf01000!FxObject::FinalRelease+0x1a**

**13 fffff285`5f9a6e00 fffff800`3050351d     Wdf01000!FxObject::Release+0x49**

**14 fffff285`5f9a6e40 fffff800`305034b8     Wdf01000!FxObject::DeletedAndDisposedWorkerLocked+0x4d**

**15 fffff285`5f9a6e80 fffff800`30503336     Wdf01000!FxObject::DeleteWorkerAndUnlock+0x58**

**16 fffff285`5f9a6eb0 fffff800`3050718b     Wdf01000!FxObject::DeleteObject+0x76**

**17 fffff285`5f9a6ee0 fffff800`660578b9     Wdf01000!imp\_WdfObjectDelete+0x4b**

**18 (Inline Function) --------`--------     NetAdapterCx!wil::details::resource\_policy<WDFWAITLOCK\_\_ \*,void (\_\_cdecl\*)(WDFWAITLOCK\_\_ \*),&WdfWaitLockRelease,wistd::integral\_constant<unsigned \_\_int64,2>,WDFWAITLOCK\_\_ \*,WDFWAITLOCK\_\_ \*,0,std::nullptr\_t>::is\_valid+0x24**

**19 (Inline Function) --------`--------     NetAdapterCx!wil::details::unique\_storage<wil::details::resource\_policy<WDFWAITLOCK\_\_ \*,void (\_\_cdecl\*)(WDFWAITLOCK\_\_ \*),&WdfWaitLockRelease,wistd::integral\_constant<unsigned \_\_int64,2>,WDFWAITLOCK\_\_ \*,WDFWAITLOCK\_\_ \*,0,std::nullptr\_t> >::{dtor}+0x24**

**1a (Inline Function) --------`--------     NetAdapterCx!NxAdapter::DestroyQueue+0x9a**

**1b (Inline Function) --------`--------     NetAdapterCx!NxAdapter::DestroyQueue+0x9a**

**1c fffff285`5f9a6f30 fffff800`660a5b23     NetAdapterCx!NetClientAdapterDestroyQueue+0xa9**

**1d fffff285`5f9a6f60 fffff800`6607d89d     NetAdapterCx!NxTxXlat::Destroy+0x1a7**

**1e fffff285`5f9a6ff0 fffff800`6607d844     NetAdapterCx!NxTxXlat::~NxTxXlat+0x25**

**1f fffff285`5f9a7020 fffff800`660a3bbc     NetAdapterCx!NxTxXlat::`scalar deleting destructor'+0x14**

**20 (Inline Function) --------`--------     NetAdapterCx!wistd::default\_delete<NxTxXlat>::operator()+0x11**

**21 (Inline Function) --------`--------     NetAdapterCx!wistd::unique\_ptr<NxTxXlat,wistd::default\_delete<NxTxXlat> >::reset+0x1f**

**22 (Inline Function) --------`--------     NetAdapterCx!wistd::unique\_ptr<NxTxXlat,wistd::default\_delete<NxTxXlat> >::{dtor}+0x1f**

**23 (Inline Function) --------`--------     NetAdapterCx!Rtl::KArray<wistd::unique\_ptr<NxTxXlat,wistd::default\_delete<NxTxXlat> >,512>::resize+0x40**

**24 (Inline Function) --------`--------     NetAdapterCx!Rtl::KArray<wistd::unique\_ptr<NxTxXlat,wistd::default\_delete<NxTxXlat> >,512>::clear+0x40**

**25 (Inline Function) --------`--------     NetAdapterCx!QueueControl::DestroyQueues+0x72**

**26 fffff285`5f9a7050 fffff800`66074c59     NetAdapterCx!NxTranslationApp::DestroyDatapath+0xd8**

**27 fffff285`5f9a70c0 fffff800`6605d079     NetAdapterCx!NetClientAdapterDestroyDatapath+0x9**

**28 fffff285`5f9a70f0 fffff800`6605dc29     NetAdapterCx!NxAdapter::DatapathDestroy+0x45**

**29 fffff285`5f9a7120 fffff800`66073318     NetAdapterCx!NxAdapterStateMachine<NxAdapter>::EntryFuncs::DatapathRestartDestroyingEntry+0x9**

**2a (Inline Function) --------`--------     NetAdapterCx!SmFx::StateMachineEngine::StateMachineEngineImpl::InvokeStateEntryFunction+0x2c**

**2b fffff285`5f9a7150 fffff800`66073b4c     NetAdapterCx!SmFx::StateMachineEngine::StateMachineEngineImpl::ExecuteCurrentState+0x84**

**2c fffff285`5f9a71d0 fffff800`66072ccf     NetAdapterCx!SmFx::StateMachineEngine::StateMachineEngineImpl::ProcessEventQueue+0x138**

**2d (Inline Function) --------`--------     NetAdapterCx!SmFx::StateMachineEngine::StateMachineEngineImpl::EnqueueEvent+0xdd**

**2e fffff285`5f9a7220 fffff800`6605583c     NetAdapterCx!SmFx::StateMachineEngine::EnqueueEvent+0xfb**

**2f (Inline Function) --------`--------     NetAdapterCx!NxAdapterStateMachine<NxAdapter>::EnqueueEvent+0xa**

**30 (Inline Function) --------`--------     NetAdapterCx!AdapterPnpPower::StopIoD3+0x26**

**31 fffff285`5f9a7260 fffff800`66073318     NetAdapterCx!AdapterPnpPowerStateMachine<AdapterPnpPower>::EntryFuncs::InterfaceStartedGoingToIoStoppedD3Entry+0x2c**

**32 (Inline Function) --------`--------     NetAdapterCx!SmFx::StateMachineEngine::StateMachineEngineImpl::InvokeStateEntryFunction+0x2c**

**33 fffff285`5f9a72a0 fffff800`66073b4c     NetAdapterCx!SmFx::StateMachineEngine::StateMachineEngineImpl::ExecuteCurrentState+0x84**

**34 fffff285`5f9a7320 fffff800`66072ccf     NetAdapterCx!SmFx::StateMachineEngine::StateMachineEngineImpl::ProcessEventQueue+0x138**

**35 (Inline Function) --------`--------     NetAdapterCx!SmFx::StateMachineEngine::StateMachineEngineImpl::EnqueueEvent+0xdd**

**36 fffff285`5f9a7370 fffff800`6605661f     NetAdapterCx!SmFx::StateMachineEngine::EnqueueEvent+0xfb**

**37 (Inline Function) --------`--------     NetAdapterCx!AdapterPnpPowerStateMachine<AdapterPnpPower>::EnqueueEvent+0xd**

**38 (Inline Function) --------`--------     NetAdapterCx!AdapterPnpPower::IoStop+0x1e**

**39 (Inline Function) --------`--------     NetAdapterCx!DevicePnpPower::PoweringDownD3::\_\_l2::<lambda\_8290f65210c314f913c9802f5c9fe611>::operator()+0x1e**

**3a (Inline Function) --------`--------     NetAdapterCx!NxCollection<NxAdapter>::ForEach+0x4f**

**3b (Inline Function) --------`--------     NetAdapterCx!DevicePnpPower::PoweringDownD3+0x56**

**3c fffff285`5f9a73b0 fffff800`66073318     NetAdapterCx!DevicePnpPowerStateMachine<DevicePnpPower>::EntryFuncs::PoweringDownD3Entry+0x6f**

**3d (Inline Function) --------`--------     NetAdapterCx!SmFx::StateMachineEngine::StateMachineEngineImpl::InvokeStateEntryFunction+0x2c**

**3e fffff285`5f9a7420 fffff800`66073b4c     NetAdapterCx!SmFx::StateMachineEngine::StateMachineEngineImpl::ExecuteCurrentState+0x84**

**3f fffff285`5f9a74a0 fffff800`66072ccf     NetAdapterCx!SmFx::StateMachineEngine::StateMachineEngineImpl::ProcessEventQueue+0x138**

**40 (Inline Function) --------`--------     NetAdapterCx!SmFx::StateMachineEngine::StateMachineEngineImpl::EnqueueEvent+0xdd**

**41 fffff285`5f9a74f0 fffff800`660560f8     NetAdapterCx!SmFx::StateMachineEngine::EnqueueEvent+0xfb**

**42 (Inline Function) --------`--------     NetAdapterCx!KWaitEventBase<wistd::integral\_constant<enum \_EVENT\_TYPE,1> >::Wait+0x5**

**43 fffff285`5f9a7530 fffff800`66066ed3     NetAdapterCx!DevicePnpPower::ChangePowerState+0x48**

**44 fffff285`5f9a7570 fffff800`3056d291     NetAdapterCx!EvtCxDevicePreD0ExitPreHardwareDisabled+0x53**

**45 fffff285`5f9a75a0 fffff800`3050ffae     Wdf01000!FxPnpDeviceD0ExitPreHwDisabled::InvokeCxCallback+0x31**

**46 fffff285`5f9a7600 fffff800`3050fef6     Wdf01000!FxPrePostCallback::IssuePreCxCallbacksStateless+0x54**

**47 fffff285`5f9a7630 fffff800`3056edec     Wdf01000!FxPrePostCallback::InvokeStateless+0x3e**

**48 (Inline Function) --------`--------     Wdf01000!FxPnpDeviceD0ExitPreHwDisabled::Invoke+0x10**

**49 fffff285`5f9a7660 fffff800`3056ec4b     Wdf01000!FxPkgPnp::PowerGotoDxIoStoppedCommon+0x48**

**4a (Inline Function) --------`--------     Wdf01000!FxPkgPnp::PowerGotoDxIoStopped+0x7**

**4b fffff285`5f9a76d0 fffff800`3056e970     Wdf01000!FxPkgPnp::PowerGotoDNotZeroIoStopped+0xb**

**4c fffff285`5f9a7700 fffff800`3056f947     Wdf01000!FxPkgPnp::PowerEnterNewState+0x194**

**4d fffff285`5f9a7840 fffff800`3056f774     Wdf01000!FxPkgPnp::PowerProcessEventInner+0x177**

**4e fffff285`5f9a78c0 fffff800`30582eb2     Wdf01000!FxPkgPnp::PowerProcessEvent+0x1c0**

**4f (Inline Function) --------`--------     Wdf01000!FxPkgFdo::LowerDevicePower+0x11**

**50 fffff285`5f9a7950 fffff800`30583241     Wdf01000!FxPkgFdo::DispatchDeviceSetPower+0xce**

**51 fffff285`5f9a79a0 fffff800`30507a94     Wdf01000!FxPkgFdo::\_DispatchSetPower+0x21**

**52 fffff285`5f9a79d0 fffff800`30507b41     Wdf01000!FxPkgPnp::Dispatch+0xd4**

**53 (Inline Function) --------`--------     Wdf01000!DispatchWorker+0x2e**

**54 (Inline Function) --------`--------     Wdf01000!FxDevice::Dispatch+0x3d**

**55 fffff285`5f9a7a40 fffff800`2d7d5321     Wdf01000!FxDevice::DispatchWithLock+0x81**

**56 fffff285`5f9a7a90 fffff800`2d60f4a7     nt!PopIrpWorker+0x261**

**57 fffff285`5f9a7b30 fffff800`2d82de84     nt!PspSystemThreadStartup+0x57**

**58 fffff285`5f9a7b80 00000000`00000000     nt!KiStartSystemThread+0x34**

**11: kd> .frame /r 8**

**08 fffff285`5f9a6d00 fffff800`660874b4     NetAdapterCx!ExecutionContext::~ExecutionContext+0x4d**

**rax=0000000000000001 rbx=ffff800f2f5ee050 rcx=ffff800f2f5ee4e8**

**rdx=0000000000000000 rsi=ffff800f2a843610 rdi=ffff800f2f5ee5f0**

**rip=fffff800660a70f9 rsp=fffff2855f9a6d00 rbp=0000000000000000**

**r8=0000000000000000  r9=ffff800f00efb040 r10=fffff8002d752680**

**r11=ffff800f00efb004 r12=0000000000000008 r13=0000000000000000**

**r14=00007ff0d57bca68 r15=0000000000000000**

**iopl=0         nv up ei ng nz na po nc**

**cs=0010  ss=0018  ds=002b  es=002b  fs=0053  gs=002b             efl=00040286**

**NetAdapterCx!ExecutionContext::~ExecutionContext+0x4d:**

**fffff800`660a70f9 cd2c            int     2Ch**

**11: kd> ub**

**NetAdapterCx!ExecutionContext::~ExecutionContext+0x29:**

**fffff800`660a70d5 e8de070000      call    NetAdapterCx!Statistics::Hub::RemoveHistogramReference (fffff800`660a78b8)**

**fffff800`660a70da 488bcb          mov     rcx,rbx**

**fffff800`660a70dd e80604feff      call    NetAdapterCx!ExecutionContext::Destroy (fffff800`660874e8)**

**fffff800`660a70e2 488d8b98040000  lea     rcx,[rbx+498h]**

**fffff800`660a70e9 4c8b150884ffff  mov     r10,qword ptr [NetAdapterCx!\_imp\_KeReadStateEvent (fffff800`6609f4f8)]**

**fffff800`660a70f0 e88bb56ac7      call    nt!FsRtlNumberOfRunsInBaseMcb (fffff800`2d752680)**

**fffff800`660a70f5 85c0            test    eax,eax**

**fffff800`660a70f7 7402            je      NetAdapterCx!ExecutionContext::~ExecutionContext+0x4f (fffff800`660a70fb)**

**11: kd> dt this m\_workerThreadRequested.m\_event.Header.SignalState**

**Local var @ rbx Type ExecutionContext\***

**+0x498 m\_workerThreadRequested                            :**

**+0x000 m\_event                                            :**

**+0x000 Header                                             :**

**+0x004 SignalState                                        : 0n1**

<https://hsdes.intel.com/appstore/article/#/14018487625>

[Win11 OS][SV3][NetCx][WWAN] SYSTEM\_THREAD\_EXCEPTION\_NOT\_HANDLED (7e) in MbbCx.sys after restart:

ndis!ndisVerifierNdisMIndicateStatusEx is dereferencing NULL pointer because ndis!ndisVerifierNdisDispatch is not initialized, which happens because nt!ViFnXdvQueryDispatchTable is not initialized either.

**2: 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: fffff8023cad1fc9, The address that the exception occurred at**

**Arg3: ffffd488fe717228, Exception Record Address**

**Arg4: ffffd488fe716a40, Context Record Address**

**2: kd> !error c0000005**

**Error code: (NTSTATUS) 0xc0000005 (3221225477) - The instruction at 0x%p referenced memory at 0x%p. The memory could not be %s.**

**2: kd> u fffff8023cad1fc9 L1**

**ndis!ndisVerifierNdisMIndicateStatusEx+0x19:**

**fffff802`3cad1fc9 488b4028        mov     rax,qword ptr [rax+28h]**

**2: kd> k**

**# Child-SP          RetAddr               Call Site**

**00 ffffd488`fe7161c8 fffff802`3acb94a2     nt!KeBugCheckEx**

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

**02 ffffd488`fe7161d0 fffff802`3ac4cff1     nt!PspSystemThreadStartup$filt$0+0x44**

**03 ffffd488`fe716210 fffff802`3aca3dcf     nt!\_\_C\_specific\_handler+0xa1**

**04 ffffd488`fe716280 fffff802`3ab296b2     nt!RtlpExecuteHandlerForException+0xf**

**05 ffffd488`fe7162b0 fffff802`3ab2888e     nt!RtlDispatchException+0x2d2**

**06 ffffd488`fe716a10 fffff802`3acae585     nt!KiDispatchException+0x1ae**

**07 ffffd488`fe7170f0 fffff802`3aca989f     nt!KiExceptionDispatch+0x145**

**08 ffffd488`fe7172d0 fffff802`3cad1fc9     nt!KiPageFault+0x45f**

**09 ffffd488`fe717460 fffff80a`6ff379fe     ndis!ndisVerifierNdisMIndicateStatusEx+0x19**

**0a ffffd488`fe7174a0 fffff80a`6ff1d60e     MbbCx!MbbUtilNdisMiniportIndicateStatusEx+0x86**

**0b (Inline Function) --------`--------     MbbCx!MbbNdisMiniportIndicateRequestStatus+0x4e**

**0c ffffd488`fe717520 fffff80a`6ff1d77b     MbbCx!MbbNdisDeviceServiceEventStatusHandler+0x216**

**0d ffffd488`fe717630 fffff80a`6ff311a1     MbbCx!MbbNdisDeviceServiceStatusHandler+0xab**

**0e ffffd488`fe717680 fffff80a`6ff10a5c     MbbCx!MbbUtilCommonCIDResponse+0xa5**

**0f ffffd488`fe7177e0 fffff80a`6ff2de98     MbbCx!MbbNdisIndicateStatus+0xbc**

**10 ffffd488`fe717840 fffff80a`6ff2d0a2     MbbCx!MbbReqFsmResponseReceived+0x68**

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

**12 ffffd488`fe717880 fffff80a`6ff10feb     MbbCx!MbbReqMgrQueueEvent+0x18e**

**13 ffffd488`fe7178f0 fffff80a`6ff113c9     MbbCx!MbbNdisParseStatusIndication+0xef**

**14 ffffd488`fe717950 fffff80a`6ff2ddad     MbbCx!MbbNdisParseResponseFragment+0x169**

**15 ffffd488`fe7179d0 fffff80a`6ff2d0a2     MbbCx!MbbReqFsmSendComplete+0x5d**

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

**17 ffffd488`fe717a00 fffff80a`6ff2cdc5     MbbCx!MbbReqMgrQueueEvent+0x18e**

**18 ffffd488`fe717a70 fffff80a`6ff30190     MbbCx!MbxMessagesHandler+0xb5**

**19 ffffd488`fe717ac0 fffff802`3ab27657     MbbCx!MbbWorkMgrProcessWorkItem+0x120**

**1a ffffd488`fe717b30 fffff802`3ac9b494     nt!PspSystemThreadStartup+0x57**

**1b ffffd488`fe717b80 00000000`00000000     nt!KiStartSystemThread+0x34**

**2: kd> u ndis!ndisVerifierNdisMIndicateStatusEx ndis!ndisVerifierNdisMIndicateStatusEx+0x19**

**ndis!ndisVerifierNdisMIndicateStatusEx:**

**fffff802`3cad1fb0 4883ec38        sub     rsp,38h**

**fffff802`3cad1fb4 488b05bd450400  mov     rax,qword ptr [ndis!ndisVerifierNdisDispatch (fffff802`3cb16578)]**

**fffff802`3cad1fbb 4c8d0d2e90f6ff  lea     r9,[ndis!NdisMIndicateStatusEx (fffff802`3ca3aff0)]**

**fffff802`3cad1fc2 4c8b8160130000  mov     r8,qword ptr [rcx+1360h]**

**fffff802`3cad1fc9 488b4028        mov     rax,qword ptr [rax+28h]**

**2: kd> dq ndis!ndisVerifierNdisDispatch  L1**

**fffff802`3cb16578  00000000`00000000**

**2: kd> dq nt!ViFnXdvQueryDispatchTable L1**

**fffff802`3b5d9a18  00000000`00000000**

<https://hsdes.intel.com/appstore/article/#/22016465928>

[MTL][A3][WinML] Pix Capture with GPU Causes BugCheck - VIDEO\_DXGKRNL\_FATAL\_ERROR:

This issue is caused by Intel(R) Movidius(TM) VPU Driver (ivdkmd.sys) - it calls DXGKCB\_SETPOWERCOMPONENTACTIVE function from its DXGKDDI\_CALIBRATEGPUCLOCK callback.

However DXGKDDI\_CALIBRATEGPUCLOCK callabck is DISPATCH\_LEVEL\_IRQL (see <https://learn.microsoft.com/en-us/windows-hardware/drivers/ddi/d3dkmddi/nc-d3dkmddi-dxgkddi_calibrategpuclock)>

while DXGKCB\_SETPOWERCOMPONENTACTIVE is PASSIVE\_LEVEL\_IRQL (see <https://learn.microsoft.com/en-us/windows-hardware/drivers/ddi/d3dkmddi/nc-d3dkmddi-dxgkcb_setpowercomponentactive).>

So this is IRQL violation and Direct X detects it and, since this is a fatal fault, has to stop the System - hence the Bugcheck.

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

**VIDEO\_DXGKRNL\_FATAL\_ERROR (113)**

**The dxgkrnl has detected that a violation has occurred. This resulted**

**in a condition that dxgkrnl can no longer progress.  By crashing, dxgkrnl**

**is attempting to get enough information into the minidump such that somebody**

**can pinpoint the crash cause. Any other values after parameter 1 must be**

**individually examined according to the subtype.**

**Arguments:**

**Arg1: 0000000000000014, The subtype of the BugCheck:**

**Arg2: ffffe50f382a7000**

**Arg3: 0000000000000000**

**Arg4: 0000000000000000**

**10: kd> k**

**# Child-SP          RetAddr               Call Site**

**00 fffff682`e0967728 fffff803`92455685     nt!KeBugCheckEx**

**01 (Inline Function) --------`--------     watchdog!WdLogEvent5+0x3a64**

**02 fffff682`e0967730 fffff803`91ff5d65     watchdog!WdLogSingleEntry5+0x3b45**

**03 fffff682`e09677e0 fffff803`91fe0fa9     dxgkrnl!DXGADAPTER::SetPowerComponentActiveCBWorker+0x23435**

**04 fffff682`e09678d0 fffff803`921a904a     dxgkrnl!DXGADAPTER::SetPowerComponentActiveCB+0x61**

**05 fffff682`e0967910 fffff803`95a04926     dxgkrnl!DxgSetPowerComponentActiveCB+0x3a**

**06 fffff682`e0967980 fffff803`959f36e5     ivdkmd+0x14926**

**07 fffff682`e09679c0 fffff803`92005f6b     ivdkmd+0x36e5**

**08 fffff682`e0967a00 fffff803`920058ce     dxgkrnl!ADAPTER\_RENDER::DdiCalibrateGpuClock+0xe3**

**09 fffff682`e0967b10 fffff803`9200945c     dxgkrnl!ADAPTER\_RENDER::PerformClockCalibration+0x92**

**0a fffff682`e0967bb0 fffff803`77ac35d9     dxgkrnl!DxgkpCalibrateGpuTimerDpc+0xc**

**0b fffff682`e0967be0 fffff803`77ac5176     nt!KiProcessExpiredTimerList+0x1e9**

**0c (Inline Function) --------`--------     nt!KiExpireTimerTable+0x31e**

**0d (Inline Function) --------`--------     nt!KiTimerExpiration+0x933**

**0e fffff682`e0967d20 fffff803`77c69905     nt!KiRetireDpcList+0xec6**

**0f fffff682`e0967fb0 fffff803`77c698af     nt!KySwapStacksAndRetireDpcList+0x5**

**10 fffff682`e4b3f950 fffff803`77a7daed     nt!KiPlatformSwapStacksAndCallReturn**

**11 fffff682`e4b3f960 fffff803`77c691db     nt!KiDispatchInterrupt+0xcd**

**12 fffff682`e4b3f9f0 fffff803`77c64b86     nt!KiDpcInterruptBypass+0x1b**

**13 fffff682`e4b3fa20 00007ffd`d09594d2     nt!KiInterruptDispatch+0xb6**

**14 0000007c`659fe4b0 00000000`00000000     0x00007ffd`d09594d2**

**10: kd> !irql**

**Debugger saved IRQL for processor 0xa -- 2 (DISPATCH\_LEVEL)**