洪先生 您好:

感谢电话沟通，经您的确认，我将暂时归档此案例。

工单的归档并不会影响我们为您提供技术支持服务，如您有其他问题，您可以致电技术支持热线 4008180055。

案例总结：

问题定义：

Windows 10 神州网信政府版 V0-H 系统发生蓝屏问题。

问题总结：

经您的确认，此故障机已经重做系统，case 将暂做归档处理。

问题分析：

这个 dump 显示蓝屏的直接原因是 RBtree 出现了损坏导致的。

bugcheck code 为 0x139，subcode 为 0x1D，表示 RTL_BALANCED_NODE RBtree 项已损坏。

进一步查看整个 RBtree 的结构，发现 root 节点的子节点为空，这里出现了问题。

```
2: kd> !mex.ddt _RTL_BALANCED_NODE fffff803717b7b30

dt _RTL_BALANCED_NODE fffff803717b7b30 () Recursive: [ -r1 -r2 -r ] Verbose Normal dt
================================================================================
nt!_RTL_BALANCED_NODE
   +0x000 Children         : [2] (null)
   +0x000 Left             : (null)
   +0x008 Right            : (null)
   +0x010 Red              : 0y1
   +0x010 Balance          : 0y01 (0n1)
   +0x010 ParentValue      : 0xfffff803`717cee61 (0n-8781304107423)
```

对于当前这个问题，RBtree 只有在使用、进行检查时才能发现它损坏了，进而触发蓝屏，而它是什么时候损坏、谁把它写坏的，当前 dump 是无法分析的。

由于仅有一个 dump，建议排查三方驱动问题。

以上，如您后续有任何问题，可随时与我们联系，谢谢。

危亮 Wei Liang
神州网信技术有限公司

C&M Information Technologies Co.,Ltd.
服务支持电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

神州网信 CMIT

发件人: Wei Liang
发送时间: 2021 年 10 月 15 日 15:28
收件人: '吴毓杰' <win10sup@sdc.icbc.com.cn>; 'hongbo@icbc.com.cn' <hongbo@icbc.com.cn>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: [案例号：CAS-04866-R7R3V8] % |P3|ICBC|工行总行蓝屏问题分析 % 初次响应 CMIT:0001547

洪先生 您好:

感谢电话沟通。

这个 dump 显示蓝屏的直接原因是 RBtree 出现了损坏导致的。

bugcheck code 为 0x139，subcode 为 0x1D，表示 RTL_BALANCED_NODE RBtree 项已损坏。

```
2: kd> !analyze -v
*******************************************************************************
*                                                                             *
*                        Bugcheck Analysis                                    *
*                                                                             *
*******************************************************************************

KERNEL_SECURITY_CHECK_FAILURE (139)
A kernel component has corrupted a critical data structure.  The corruption
could potentially allow a malicious user to gain control of this machine.
Arguments:
Arg1: 000000000000001d, Type of memory safety violation
Arg2: ffff850d7b63f5e0, Address of the trap frame for the exception that caused the bugcheck
Arg3: ffff850d7b63f538, Address of the exception record for the exception that caused the bugcheck
Arg4: 0000000000000000, Reserved
```

```
TRAP_FRAME:  ffff850d7b63f5e0 -- (.trap 0xffff850d7b63f5e0)
NOTE: The trap frame does not contain all registers.
Some register values may be zeroed or incorrect.
rax=0000000000000000 rbx=0000000000000000 rcx=000000000000001d
rdx=fffff803717cee60 rsi=0000000000000000 rdi=0000000000000000
rip=fffff803715034b5 rsp=ffff850d7b63f770 rbp=0000000000000001
 r8=fffff803717b7b30  r9=0000000000000000 r10=fffff803717ffb48
r11=fffff803717b7b30 r12=0000000000000000 r13=0000000000000000
r14=0000000000000000 r15=0000000000000000
iopl=0         nv up ei pl nz na po cy
nt!RtlRbInsertNodeEx+0x325:
fffff803`715034b5 cd29            int     29h
Resetting default scope

EXCEPTION_RECORD:  ffff850d7b63f538 -- (.exr 0xffff850d7b63f538)
ExceptionAddress: fffff803715034b5 (nt!RtlRbInsertNodeEx+0x0000000000000325)
   ExceptionCode: c0000409 (Security check failure or stack buffer overrun)
  ExceptionFlags: 00000001
NumberParameters: 1
   Parameter[0]: 000000000000001d
Subcode: 0x1d FAST_FAIL_INVALID_BALANCED_TREE
```

查看当前 Callstack 和 RbInsertNode 操作所在的 frame 情况。

```
2: kd> k
 # Child-SP          RetAddr           Call Site
00 ffff850d`7b63f2b8 fffff803`715d66a9 nt!KeBugCheckEx
01 ffff850d`7b63f2c0 fffff803`715d6a50 nt!KiBugCheckDispatch+0x69
02 ffff850d`7b63f400 fffff803`715d5065 nt!KiFastFailDispatch+0xd0
03 ffff850d`7b63f5e0 fffff803`715034b5 nt!KiRaiseSecurityCheckFailure+0x2e5
04 ffff850d`7b63f770 fffff803`71420a26 nt!RtlRbInsertNodeEx+0x325
05 ffff850d`7b63f780 fffff803`71663ba0 nt!KiSetClockInterval+0xa6
06 ffff850d`7b63f7b0 fffff803`71663bd4 nt!KiSetVirtualHeteroClockIntervalRequest+0x50
07 ffff850d`7b63f7e0 fffff803`71522b67 nt!KiSetVirtualHeteroClockIntervalRequestDpcRoutine
08 ffff850d`7b63f810 fffff803`715221bb nt!KiExecuteAllDpcs+0x2e7
09 ffff850d`7b63f950 fffff803`715c91ca nt!KiRetireDpcList+0x1db
0a ffff850d`7b63fb60 00000000`00000000 nt!KiIdleLoop+0x5a
2: kd> .frame /r 04;
04 ffff850d`7b63f770 fffff803`71420a26 nt!RtlRbInsertNodeEx+0x325
rax=0000000000000000 rbx=0000000000000040 rcx=000000000000001d
rdx=fffff803717cee60 rsi=0000000000000000 rdi=0000000000000001
rip=fffff803715034b5 rsp=ffff850d7b63f770 rbp=0000000000000001
 r8=fffff803717b7b30  r9=0000000000000000 r10=fffff803717ffb48
r11=fffff803717b7b30 r12=0000000000000000 r13=0000000000000000
r14=0000000000000000 r15=0000000000000001
iopl=0         nv up ei ng nz na po nc
cs=0010  ss=0018  ds=002b  es=002b  fs=0053  gs=002b             efl=00000286
nt!RtlRbInsertNodeEx+0x325:
fffff803`715034b5 cd29            int     29h
```

进一步查看整个 RBtree 的结构，发现 root 节点的子节点为空，这里出现了问题。

```
2: kd> !mex.ddt _RTL_BALANCED_NODE fffff803717b7b30

dt _RTL_BALANCED_NODE fffff803717b7b30 () Recursive: [ -r1 -r2 -r ] Verbose Normal dt
================================================================================
nt!_RTL_BALANCED_NODE
   +0x000 Children             : [2] (null)
   +0x000 Left                 : (null)
   +0x008 Right                : (null)
   +0x010 Red                  : 0y1
   +0x010 Balance              : 0y01 (0n1)
   +0x010 ParentValue          : 0xfffff803`717cee61 (0n-8781304107423)
```

dump 文件是在进行转储那一时刻的快照。 它显示了正在执行的进程以及已加载的模块，记录了系统转储那一时刻的状态。

对于当前这个问题，RBtree 只有在使用、进行检查时才能发现它损坏了，进而触发蓝屏，而它是什么时候损坏、谁把它写坏的，当前 dump 是无法分析的。

由于仅有一个 dump，**建议排查三方驱动**问题。

建议方案：

如果不能提供多个 dump，建议测试移除 DSPClient、亚信等三方驱动，观察运行情况。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

发件人: Wei Liang
发送时间: 2021 年 10 月 13 日 14:43
收件人: 吴毓杰 <win10sup@sdc.icbc.com.cn>; 'hongbo@icbc.com.cn' <hongbo@icbc.com.cn>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: [案例号：CAS-04866-R7R3V8] % |P3|ICBC|工行总行蓝屏问题分析 % 初次响应 CMIT:0001547

洪先生 您好:

我谨在此阐述我们双方针对这个问题所涉及范围界定:

问题定义:

Windows 10 神州网信政府版 V0-H 系统发生蓝屏问题。

问题范围:

我们将协助您分析处理上述问题，并对定义的问题给予最大的技术支持。

如果能及时解决问题，或问题属于产品设计的行为，或问题涉及到三方，我们将考虑关闭案例。如果存在多个问题，则我们考虑拆分案例进行分析。

接下来，我们将开始合作解决这个问题。如果您对以上的问题范围界定有任何异议，请尽快告知。如果您有其他任何疑问。也欢迎随时与我联系。

案例进展：

目前正在分析 dump 日志过程中，如果有进展我将第一时间与您沟通。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

发件人: Wei Liang <weiliang@cmgos.com>
发送时间: 2021 年 10 月 12 日 17:37
收件人: 吴毓杰 <win10sup@sdc.icbc.com.cn>
抄送: Wei Liang <weiliang@cmgos.com>
主题: [案例号：CAS-04866-R7R3V8]％ |P3|ICBC|工行总行蓝屏问题分析 ％初次响应 CMIT:0001547

吴毓杰 先生/女士，您好!

感谢您联系神州网信技术支持中心。 我是技术支持工程师 危亮 。 很高兴能有机会协助您解决该问题。 您可随时通过邮件回复以及该问题事件号码 CAS-04866-R7R3V8 与我联系。

如果您有任何其他疑问，请随时与我联系。

此致,

敬礼
