许先生 您好:

感谢您的回复。

经过您的确认，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，如有其他问题，您可以随时联系我们。

案例总结：

问题定义：

用户反馈罗总的设备在内网环境下出现异常蓝屏问题，需要协助分析。

问题总结：

获取的两个 minidump 文件，一个显示蓝屏问题与 vwifimf.sys 有关，需要三方应用厂商排查 vwifimf 驱动。另一个显示可能文件系统出现问题，建议通过 chkdsk /f /r c: 命令检测系统盘文件系统情况。

minidump 中的信息有限，建议配置 fulldump 后，当再次出现问题时获取完整的内存转储信息进一步分析。

当前领导设备暂无法获取 full dump 文件，同意归档案例。

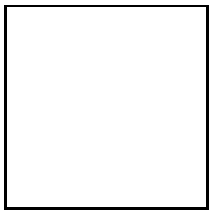
以上，如您后续有任何问题，可随时与我们联系，谢谢。

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: Soul power ギ <303642690@qq.com>
发送时间: 2023 年 9 月 26 日 11:07
收件人: Wei Liang <weiliang@cmgos.com>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: 回复: [案例号: CAS-09919-G6W4S6] % |P1|ICBC|win10 政府版 1809 在内网环境下持续异常蓝屏 % 初次响应 CMIT:0001428

工程师，您好，此问题日志暂无法获取，请先归档。



Soul power ギ
303642690@qq.com

---------- 原始邮件 ----------

发件人: "Wei Liang" <weiliang@cmgos.com>;

发送时间: 2023 年 9 月 22 日(星期五) 下午 4:25

收件人: "Soul power ギ"<303642690@qq.com>;

抄送: "ICBC_Notification"<ICBC_Notification@cmgos.com>;

主题: 回复:[案例号: CAS-09919-G6W4S6] % |P1|ICBC|win10 政府版 1809 在内网环境下持续异常蓝屏 % 初次响应 CMIT:0001428

许先生 您好:

感谢您的电话接听。

如电话中所说，当前领导设备暂无法获取 full dump 文件，也未再次复现蓝屏问题，需观察一段时间确认后续是否再次出现同样问题。

如果有任何进展或疑问可以回复此邮件。

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: 2023 年 9 月 21 日 15:56
收件人: 许翔 <303642690@qq.com>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: [案例号：CAS-09919-G6W4S6] % |P1|ICBC|win10 政府版 1809 在内网环境下持续异常蓝屏 % 初次响应 CMIT:0001428

许先生 您好:

感谢您的电话接听。

根据您提供的信息，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:

用户反馈罗总的设备在内网环境下出现异常蓝屏问题，需要协助分析。

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。

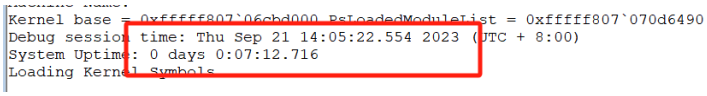
如果能及时解决问题，或问题属于产品设计的行为，或问题涉及到三方，我们将考虑关闭案例。如果存在多个问题，则我们考虑拆分案例进行分析。

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。

针对您提供的两个 mini dump 文件，具体分析如下：

092123-20265-01.dmp 文件：

显示在开机 7 分 12 秒后，在 14:05 出现蓝屏问题。



蓝屏报错代码为 0x139，这指示内核已检测到关键数据结构的损坏。

```
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: 0000000000000003, A LIST_ENTRY has been corrupted (i.e. double remove).
Arg2: ffffb183dc40f1f0, Address of the trap frame for the exception that caused the bugcheck
Arg3: ffffb183dc40f148, Address of the exception record for the exception that caused the bugcheck
Arg4: 0000000000000000, Reserved

Debugging Details:
------------------
```

查看对应的 call stack 信息，显示有 ntfs 和 fltmgr 驱动参与。

```
2: kd> knL
 # Child-SP          RetAddr           Call Site
00 ffffb183`dc40eec8 fffff807`06e89d29 nt!KeBugCheckEx
01 ffffb183`dc40eed0 fffff807`06e8a210 nt!KiBugCheckDispatch+0x69
02 ffffb183`dc40f010 fffff807`06e88288 nt!KiFastFailDispatch+0xd0
03 ffffb183`dc40f1f0 fffff807`0735e527 nt!KiRaiseSecurityCheckFailure+0x308
04 ffffb183`dc40f380 fffff807`0a5bb11f nt!FsRtlTeardownPerFileContexts+0xc7
05 ffffb183`dc40f3c0 fffff807`0a4df2cf Ntfs!NtfsDeleteFcb+0x3df
06 ffffb183`dc40f440 fffff807`0a5bb57b Ntfs!NtfsTeardownFromLcb+0x3cf
07 ffffb183`dc40f4e0 fffff807`0a4e23f3 Ntfs!NtfsTeardownStructures+0xeb
08 ffffb183`dc40f560 fffff807`0a5bf1a3 Ntfs!NtfsDecrementCloseCounts+0xf3
09 ffffb183`dc40f5c0 fffff807`0a5a1b20 Ntfs!NtfsCommonClose+0xac3
0a ffffb183`dc40f690 fffff807`06ce9f49 Ntfs!NtfsFsdClose+0x2c0
0b ffffb183`dc40f7a0 fffff807`0aef77ce nt!IofCallDriver+0x59
0c ffffb183`dc40f7e0 fffff807`0aef6140 FLTMGR!FltpLegacyProcessingAfterPreCallbacksCompleted+0x28e
0d ffffb183`dc40f850 fffff807`06ce9f49 FLTMGR!FltpDispatch+0xb6
0e ffffb183`dc40f8b0 fffff807`072868a9 nt!IofCallDriver+0x59
```

当前是 mini dump，没有更详细的信息。

092123-20859-01.dmp 文件：

显示在开机 1 分 29 秒后，在 13:56 出现蓝屏问题。

```
Kernel base = 0xfffff801`48806000 PsLoadedModuleList = 0xfffff801`48c1f490
Debug session time: Thu Sep 21 13:56:01.835 2023 (UTC + 8:00)
System Uptime: 0 days 0:01:29.953
Loading Kernel Symbols
```

蓝屏报错代码为 0x50，这这表明引用了无效的系统内存。 通常，内存地址错误或内存地址指向已释放的内存。

```
*******************************************************************************
*                                                                             *
*                        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: ffffffffffffffe8, memory referenced.
Arg2: 0000000000000000, value 0 = read operation, 1 = write operation.
Arg3: fffff8014d1a94fd, If non-zero, the instruction address which referenced the bad memory
      address.
Arg4: 0000000000000002, (reserved)

Debugging Details:
------------------
```

查看对应的 call stack 信息，显示 nwifi!Dot11SendCompletion 处理 NBL 时出现异常，对应的 NBL 为 ffff8f048deeac30。

```
1: kd> knL
 # Child-SP          RetAddr           Call Site
00 ffffb788`c446c888 fffff801`48a33fcf nt!KeBugCheckEx
01 ffffb788`c446c890 fffff801`4885ab18 nt!MiSystemFault+0x13b20f
02 ffffb788`c446c9d0 fffff801`489ce903 nt!MmAccessFault+0x1d8
03 ffffb788`c446cb70 fffff801`4d1a94fd nt!KiPageFault+0x343
04 ffffb788`c446cd00 fffff801`4d1ad66d nwifi!Dot11SendCompletion+0x35
05 ffffb788`c446cd40 fffff801`4c256a13 nwifi!Tx6SendComplete+0x1d
06 ffffb788`c446cd70 fffff801`4c258c2e ndis!ndisCallSendCompleteHandler+0x33
07 ffffb788`c446cdb0 fffff801`488bd818 ndis!ndisDataPathExpandStackCallback+0x3e
08 ffffb788`c446ce00 fffff801`488bd78d nt!KeExpandKernelStackAndCalloutInternal+0x78
09 ffffb788`c446ce70 fffff801`4c27e940 nt!KeExpandKernelStackAndCalloutEx+0x1d
0a ffffb788`c446ceb0 fffff801`4dbe1f92 ndis!NdisFSendNetBufferListsComplete+0x29290
0b ffffb788`c446cfa0 ffff8f04`85bdbd01 vwifimf+0x1f92
0c ffffb788`c446cfa8 ffff8f04`8a848030 0xffff8f04`85bdbd01
0d ffffb788`c446cfb0 fffff801`00000000 0xffff8f04`8a848030
0e ffffb788`c446cfb8 00000000`00000000 0xfffff801`00000000
1: kd> .frame /r 4
04 ffffb788`c446cd00 fffff801`4d1ad66d nwifi!Dot11SendCompletion+0x35
rax=0000000000000000 rbx=ffffffffffffffe8 rcx=ffff8f048f2f81c0
rdx=ffff8f048deeac30 rsi=ffff8f048deeac30 rdi=ffff8f048f2f8200
rip=fffff8014d1a94fd rsp=ffffb788c446cd00 rbp=0000000000000000
 r8=0000000000000000  r9=0000000000000098 r10=ffff8f04897ab230
r11=0000000000000001 r12=0000000000000000 r13=0000000000000002
r14=fffff8014c258bf0 r15=0000000000000000
iopl=0         nv up ei pl zr na po nc
cs=0010  ss=0018  ds=002b  es=002b  fs=0053  gs=002b             efl=00000246
nwifi!Dot11SendCompletion+0x35:
fffff801`4d1a94fd 488b03          mov     rax,qword ptr [rbx] ds:002b:ffffffff`ffffffe8=????????????????
```

这个 NBL 是 vwifimf.sys 申请的，在 FilterSendCompleted 时，并没有正常完成并释放 NBL，反而传给了 nwifi 导致错误蓝屏。

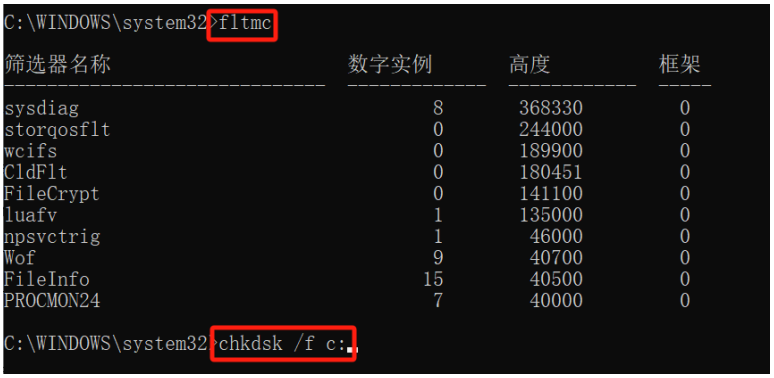
```
1: kd> !nbl ffff8f048deeac30
    NBL                 ffff8f048deeac30    Next NBL            NULL
    First NB            ffff8f048deeadb0    Source              ffff8f0489bd8a0 - Intel(R) Dual Band Wireless-AC 8265-NDIS Sample LightWeight Filter 1-000
    Context stack       ffff8f048f2f81c0    Pool                ffff8f0489bde5c0 -
    Flags               NBL ALLOCATED, NBL CONTEXT ALLOCATED

    Walk the NBL chain                      Dump data payload
    Show out-of-band information            Show in Microsoft Network Monitor

1: kd> !ndiskd.nblpool ffff8f0489bde5c0


NBL POOL

    Ndis handle         ffff8f0489bde5c0
    Allocation tag      Filt
    Owner
    Allocated by        vwifimf+1809

    Flags               CONTAINS NET BUFFER
    Structure size      0n560
    Context size        0
    Data size           0

    All allocated NBLs
```

下一步排查建议：

1）Minidump 中的信息有限，还是建议配置 fulldump 后，当再次出现问题时获取完整的内存转储信息进一步分析。

2）092123-20859-01.dmp 文件显示蓝屏问题与 vwifimf.sys 有关，请 vwifimf 厂商排查 vwifimf 未释放其申请的 NBL 原因。

3）092123-20265-01.dmp 文件显示问题可能与当前设备的文件系统有关，建议以管理员权限打开 cmd 命令行，执行 **chkdsk /f c:** 检查 C 盘系统盘的文件系统情况，并执行 **fltmc** 查看加载的 filter 驱动情况。



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 <weiliang@cmgos.com>
发送时间: 2023 年 9 月 21 日 14:52
收件人: 许翔 <303642690@qq.com>
抄送: Wei Liang <weiliang@cmgos.com>
主题: [案例号: CAS-09919-G6W4S6] % |P1|ICBC|win10 政府版 1809 在内网环境下持续异常蓝屏 % 初次响应 CMIT:0001428

许翔 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-09919-G6W4S6 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