毓杰，您好：

经内部确认，鉴于目前此 case 无更新的进度，将暂做归档处理，以下为案例总结，请您知悉：

Case No：CAS-02871-P0T5L9

问题描述：

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

用户反馈 CMGE 系统，在使用无线环境下蓝屏。需要与通软公司协助分析 nwifi 等蓝屏问题。

问题分析：

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

针对此次蓝屏问题，在分析多个 dump 之后，目前导致大部分蓝屏的问题原因仍锁定在 vwifimf 上，需要通软公司进行代码层的分析处理。

问题总结：

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

鉴于目前用户方暂时无跟进需求，同意暂时归档此 case。

以上，如您后续有任何问题，可随时与我们联系，谢谢。

李琦 Li Qi
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务电话： 4008180055
电子邮箱 Email: liqi@cmgos.com

神州网信
CMIT

发件人: Li Qi
发送时间: 2020 年 9 月 3 日 18:54
收件人: '吴毓杰' <win10sup@sdc.icbc.com.cn>; 'liyue@sdc.icbc.com.cn' <liyue@sdc.icbc.com.cn>

抄送: CRM Case Email <casemail@cmgos.com>; Liu Wei <liuwei@cmgos.com>; Li Xin <lixin@cmgos.com>; Qi Feng <qifeng@cmgos.com>; Wang Dan <wangdan@cmgos.com>; Wang Wenlei <wangwl@cmgos.com>
主题: [案例号：CAS-02871-P0T5L9] % lP2lICBCl协助通软公司分析政府版系统蓝屏问题 % 初次响应 CMIT:0001871

毓杰，您好：

此次蓝屏与之前所遇的蓝屏问题，原因不同，是一个新的问题，即内存页表文件地址非法，造成的原因可能性比较多。如下是针对这次 0x1a dump 的分析：

1. 这个 bugcheck 的发生原因是访问内存地址 PTE 时，发现内存地址非法。

```
0: kd> !crash
Dump Info
============================================
Dump Name: MEMORY.DMP
Windows 10 Kernel Version 17134 MP (4 procs) Free x64
Product: WinNt, suite: TerminalServer SingleUserTS
Edition build lab: 17134.1.amd64fre.rs4_release.180410-1804
Kernel base = 0xfffff800`8f818000 PsLoadedModuleList = 0xfffff800`8fbc4ce0
Debug session time: Wed Sep  2 12:14:01.152 2020 (UTC + 8:00)
System Uptime: 0 days 18:30:50.615
SystemManufacturer = LENOVO
SystemProductName = 20JTS2LF00
Processor: Intel(R) Core(TM) i5-6200U CPU @ 2.30GHz
Bugcheck: 1A (61941, FFFFB60B23514D88, 9, FFFF83057E2DEED0)
Kernel Complete Dump File: Full address space is available.


Bugcheck details
============================================
MEMORY_MANAGEMENT (1a)
  # Any other values for parameter 1 must be individually examined.
Arguments:
Arg1: 0000000000061941, The subtype of the bugcheck.
Arg2: ffffb60b23514d88
Arg3: 0000000000000009
Arg4: ffff83057e2deed0


Crashing Stack
============================================
Process                    Thread         CID       UserTime KernelTime ContextSwitches Wait
Reason Time State
TmListen.exe (ffffb60b26ac4580) ffffb60b23ae8400 1898.5c8       0s        0s           102
UserRequest   0s Running on CPU 0

Irp List:
    IRP             File                                            Driver
    ffffb60b290245f0 \Program Files (x86)\Asiainfo Security\OfficeScan Client\HLog
FltMgr


# Child-SP          RetAddr               Call Site
00 ffff8305`7e2ded58 fffff800`8f9e2040     nt!KeBugCheckEx
01 ffff8305`7e2ded60 fffff800`8f9d01e0     nt!MmAccessFault+0x1aed20
02 ffff8305`7e2deed0 fffff800`8fa3df20     nt!KiPageFault+0x320
03 ffff8305`7e2df060
fffff80c`ad1995ff     nt!FsRtlLookupPerStreamContextInternal+0xa0
04 ffff8305`7e2df090 fffff80c`ad1c8b6a     FLTMGR!FltpGetStreamListCtrl+0x6f
05 ffff8305`7e2df100 fffff80c`ad197751     FLTMGR!FltpCacheCreateNames+0x52
06 ffff8305`7e2df190
fffff80c`ad1cbdad     FLTMGR!FltpLegacyProcessingAfterPreCallbacksCompleted+0x6a1
07 ffff8305`7e2df200 fffff800`8f97faea     FLTMGR!FltpCreate+0x2dd
08 ffff8305`7e2df2b0 fffff800`90029b04     nt!IopfCallDriver+0x56
09 ffff8305`7e2df2f0 fffff800`8fa23aed     nt!IovCallDriver+0x50
0a ffff8305`7e2df330 fffff800`8fdc9963     nt!IofCallDriver+0x10e51d
0b (Inline Function) --------`--------     nt!IoCallDriverWithTracing+0x29
0c ffff8305`7e2df370 fffff800`8fdbdccb     nt!IopParseDevice+0x773
0d ffff8305`7e2df540 fffff800`8fdc428f     nt!ObpLookupObjectName+0x73b
0e ffff8305`7e2df720 fffff800`8fd0b9c5     nt!ObOpenObjectByNameEx+0x1df
0f ffff8305`7e2df860 fffff800`8fd0b528     nt!IopCreateFile+0x3f5
10 ffff8305`7e2df900 fffff800`8f9d3143     nt!NtOpenFile+0x58
11 ffff8305`7e2df990 00007ff9`e00db004     nt!KiSystemServiceCopyEnd+0x13
12 00000000`7391f168 00007ff9`dd26e193     ntdll!ZwOpenFile+0x14
13 00000000`7391f170 00007ff9`dd2a37a0     KERNELBASE!FindFirstFileExW+0x1c3
14 00000000`7391f530 00007ff6`7689ccbd     KERNELBASE!FindFirstFileA+0x60
15 00000000`7391f810 00000000`00000000     tmlisten+0x1eccbd
```

2. 从 call stack 来看这个非法地址来自 FSRTL_ADVANCED_FCB_HEADER，这个结构本身都是正确的，以及其他的子结构地址都正确。

```
((ntkrnlmp!_FSRTL_ADVANCED_FCB_HEADER *)0xffffa000c13eeb30)              :
0xffffa000c13eeb30 [Type: _FSRTL_ADVANCED_FCB_HEADER *]
    [+0x000] NodeTypeCode     : 1795 [Type: short]
    [+0x002] NodeByteSize     : 744 [Type: short]
    [+0x004] Flags            : 0x40 [Type: unsigned char]
    [+0x005] IsFastIoPossible : 0x0 [Type: unsigned char]
    [+0x006] Flags2           : 0x2 [Type: unsigned char]
    [+0x007 ( 3: 0)] Reserved         : 0x0 [Type: unsigned char]
    [+0x007 ( 7: 4)] Version          : 0x3 [Type: unsigned char]
    [+0x008] Resource         : 0xffffb60b297765e0 [Type: _ERESOURCE *]
    [+0x010] PagingIoResource : 0x0 [Type: _ERESOURCE *]
    [+0x018] AllocationSize   : {4096} [Type: _LARGE_INTEGER]
    [+0x020] FileSize         : {4096} [Type: _LARGE_INTEGER]
    [+0x028] ValidDataLength  : {4096} [Type: _LARGE_INTEGER]
    [+0x030] FastMutex        : 0xffffb60b297765a8 [Type: _FAST_MUTEX *]
    [+0x038] FilterContexts   [Type: _LIST_ENTRY]                    非法地址来自这里
    [+0x048] PushLock         [Type: _EX_PUSH_LOCK]
    [+0x050] FileContextSupportPointer : 0xffffa000c13eeb18 [Type: void * *]
    [+0x058] Oplock           : 0x0 [Type: void *]
    [+0x058] ReservedForRemote : 0x0 [Type: void *]
    [+0x060] ReservedContext  : 0x0 [Type: void *]

0: kd> !pool 0xffffa000c13eeb30
Pool page ffffa000c13eeb30 region is Paged pool
ffffa000c13ee000 size:  360 previous size:    0  (Allocated)  AlMs
ffffa000c13ee360 size:   10 previous size:  360  (Free)       Free
ffffa000c13ee370 size:   b0 previous size:   10  (Allocated)  TMMA
ffffa000c13ee420 size:  560 previous size:   b0  (Allocated)  Ntff
ffffa000c13ee980 size:   50 previous size:  560  (Allocated)  MiSn
*ffffa000c13ee9d0 size:  630 previous size:   50  (Allocated) *NtfF
        Pooltag NtfF : FCB_INDEX, Binary : ntfs.sys
```

3. 经查询发现这个 list 是个 empty list，因为 Flink/Blink 是一样的，本身这个 list header 理论上应是一个 nonpaged pool, OS 初始化以后是不会去释放它的。

```
0: kd> dx -r1 (*((ntkrnlmp!_LIST_ENTRY *)0xffffa000c13eeb68))
(*((ntkrnlmp!_LIST_ENTRY *)0xffffa000c13eeb68))              [Type: _LIST_ENTRY]
    [+0x000] Flink          : 0xffffb60b23514d78 [Type: _LIST_ENTRY *]
    [+0x008] Blink          : 0xffffb60b23514d78 [Type: _LIST_ENTRY *]
```

4. 同时查看这个 list 前面的一个 pool 地址,也没有写越界的迹象。再看一下 PTE 的内容，发现错误的 hardware page 地址

```
0: kd> !pool ffffb60b`23514d88
Pool page ffffb60b23514d88 region is Nonpaged pool
Page 800374a too large to be in the dump file.
ffffb60b23514000 is not a valid large pool allocation, checking large session pool...
ffffb60b23514000 is not valid pool. Checking for freed (or corrupt) pool
Address ffffb60b23514000 could not be read. It may be a freed, invalid or paged out
page

0: kd> !pool ffffb60b23514000-100
Pool page ffffb60b23513f00 region is Nonpaged pool
ffffb60b23513000 size:  810 previous size:    0  (Allocated)  IWJQ
ffffb60b23513810 size:   30 previous size:  810  (Allocated)  IWXH
ffffb60b23513840 size:   40 previous size:   30  (Allocated)  NDwi
ffffb60b23513880 size:   20 previous size:   40  (Allocated)  fbDm
ffffb60b235138a0 size:  190 previous size:   20  (Allocated)  IWQW
*ffffb60b23513a30 size:  5d0 previous size:  190  (Allocated) *Prcr
        Pooltag Prcr : Processr driver allocations, Binary : processr.sys
```

```
ffffb60b`23513f30  7965ef6c 00000659 cabcf582 0000060c  l.eyY...........
ffffb60b`23513f40  db233c00 000009a4 dc21a785 000009b1  .<#.......!.....
ffffb60b`23513f50  00000000 00000000 00000000 00000000  ................
ffffb60b`23513f60  b07a8270 fffff80c 2350dbe0 ffffb60b  p.z.......P#....
ffffb60b`23513f70  00000000 00000000 00000000 00000000  ................
ffffb60b`23513f80  00000000 00000000 00000000 00000000  ................
ffffb60b`23513f90  00000000 00000000 00000000 00000000  ................
ffffb60b`23513fa0  00000000 00000000 00000000 00000000  ................
0: kd>
ffffb60b`23513fb0  05030313 00000000 00000000 00000000  ................
ffffb60b`23513fc0  00000000 00000000 b07a7fd0 fffff80c  ..........z.....
ffffb60b`23513fd0  227296b0 ffffb60b 00000000 00000000  ..r"............
ffffb60b`23513fe0  00000000 00000000 00000000 00000000  ................
ffffb60b`23513ff0  235361d0 ffffb60b 00000000 00000000  .aS#............
Page 800374a too large to be in the dump file.
ffffb60b`23514000  ???????? ???????? ???????? ????????  ????????????????
ffffb60b`23514010  ???????? ???????? ???????? ????????  ????????????????
ffffb60b`23514020  ???????? ???????? ???????? ????????  ????????????????
0: kd>
Page 800374a too large to be in the dump file.
ffffb60b`23514030  ???????? ???????? ???????? ????????  ????????????????
ffffb60b`23514040  ???????? ???????? ???????? ????????  ????????????????
ffffb60b`23514050  ???????? ???????? ???????? ????????  ????????????????
ffffb60b`23514060  ???????? ???????? ???????? ????????  ????????????????
ffffb60b`23514070  ???????? ???????? ???????? ????????  ????????????????
ffffb60b`23514080  ???????? ???????? ???????? ????????  ????????????????
ffffb60b`23514090  ???????? ???????? ???????? ????????  ????????????????
ffffb60b`235140a0  ???????? ???????? ???????? ????????  ????????????????

0: kd> !pte ffffb60b`23513ff0
                                           VA ffffb60b23513ff0
PXE at FFFF80C060301B60    PPE at FFFF80C06036C160    PDE at
FFFF80C06D82C8D0    PTE at FFFF80DB0591A898
contains 0A00000003A44863  contains 0A00000003A45863  contains
0A00000087BEB863  contains 8A00000000649863
pfn 3a44      ---DA--KWEV  pfn 3a45      ---DA--KWEV  pfn 87beb     ---DA--KWEV  pfn
649       ---DA--KW-V

0: kd> dc FFFF80DB0591A898
ffff80db`0591a898  00649863 8a000000 0374aa63 8a000080  c.d.....c.t.....
ffff80db`0591a8a8  5554b863 8a000002 4edf0863 8a000002  c.TU....c..N....
ffff80db`0591a8b8  035ef863 8a000000 0374e863 8a000000  c.^.....c.t.....
ffff80db`0591a8c8  036b0863 8a000000 03750863 8a000000  c.k.....c.u.....
ffff80db`0591a8d8  036b1863 8a000000 03752863 8a000000  c.k.....c(u.....
ffff80db`0591a8e8  036b2863 8a000000 07754863 8a000000  c(k.....cHu.....
ffff80db`0591a8f8  88bb4a63 8a000000 88c56a63 8a000000  cJ......cj......
ffff80db`0591a908  88c57863 8a000000 496f2863 8a000002  cx......c(oI....
0: kd> !dd  00649000
```

```
#  649000 02810000 514a5749 54efca37 41ce6dca
#  649010 23513058 ffffb60b 23513070 ffffb60b
#  649020 00000000 00000000 00000000 00000000
#  649030 00000000 00000000 23513010 ffffb60b
#  649040 00000800 00000000 22574010 ffffb60b
#  649050 00000004 00000000 00000000 00000000
#  649060 00000000 00000000 00000000 00000000
#  649070 00000000 00000000 00000000 00000000
0: kd> dc ffffb60b`23513ff0
ffffb60b`23513ff0  235361d0 ffffb60b 00000000 00000000  .aS#...........



0: kd> !pte ffffb60b`23514d88
                                           VA ffffb60b23514d88
PXE at FFFF80C060301B60    PPE at FFFF80C06036C160    PDE at
FFFF80C06D82C8D0    PTE at FFFF80DB0591A8A0
contains 0A00000003A44863  contains 0A00000003A45863  contains
0A00000087BEB863  contains 8A0000800374AA63
pfn 3a44      ---DA--KWEV  pfn 3a45      ---DA--KWEV  pfn 87beb     ---DA--KWEV  pfn
800374a   C--DA--KW-V

0: kd> !dd 800374a000
Page 800374a too large to be in the dump file.
Physical memory read at 800374a000 failed
If you know the caching attributes used for the memory,
try specifying [c], [uc] or [wc], as in !dd [c] <params>.
WARNING: Incorrect use of these flags will cause unpredictable
processor corruption.  This may immediately (or at any time in
the future until reboot) result in a system hang, incorrect data
being displayed or other strange crashes and corruption.


0: kd> !pte ffffb60b`23514000
                                           VA ffffb60b23514000
PXE at FFFF80C060301B60    PPE at FFFF80C06036C160    PDE at
FFFF80C06D82C8D0    PTE at FFFF80DB0591A8A0
contains 0A00000003A44863  contains 0A00000003A45863  contains
0A00000087BEB863  contains 8A0000800374AA63
pfn 3a44      ---DA--KWEV  pfn 3a45      ---DA--KWEV  pfn 87beb     ---DA--KWEV  pfn
800374a   C--DA--KW-V

0: kd> dc FFFF80DB0591A8A0
ffff80db`0591a8a0  0374aa63 8a000080 5554b863 8a000002  c.t.....c.TU....
ffff80db`0591a8b0  4edf0863 8a000002 035ef863 8a000000  c..N....c.^.....
ffff80db`0591a8c0  0374e863 8a000000 036b0863 8a000000  c.t.....c.k.....
ffff80db`0591a8d0  03750863 8a000000 036b1863 8a000000  c.u.....c.k.....
ffff80db`0591a8e0  03752863 8a000000 036b2863 8a000000  c(u.....c(k.....
ffff80db`0591a8f0  07754863 8a000000 88bb4a63 8a000000  cHu.....cJ......
ffff80db`0591a900  88c56a63 8a000000 88c57863 8a000000  cj......cx......
ffff80db`0591a910  496f2863 8a000002 4caf1863 8a000002  c(oI....c..L....

0: kd> !dd  0374a000
# 374a000 02810000 514a5749 00000000 00000000
# 374a010 23514058 ffffb60b 23514070 ffffb60b
# 374a020 00000000 00000000 00000000 00000000
# 374a030 00000000 00000000 23514010 ffffb60b
# 374a040 00000800 00000000 22574010 ffffb60b
# 374a050 00000004 00000000 00000000 00000000
# 374a060 00000000 00000000 00000000 00000000
# 374a070 00000000 00000000 00000000 00000000
```

建议

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

我们无法再额外 trace 内存映射表这部分内容，所以无法定位查找是谁写坏的，根据我们之前的经验，一般是 firmware（bios/网卡）才会 touch 这块，或者少数的 case，最后的解决方案是卸载了杀毒软件解决的。

由于没有正面 debug 的方法，我们建议如下：

1. 了解一下问题发生之前的改动，是否有 firmware/storage/network 控制器的升级动作，有个话请降级。
2. 如果没有变动，请先升级 firmware，包含系统/网卡/存储
3. 基于目前工行的软件安装情况，为方便进一步分析此问题，如果条件允许的话，请卸载相关的安控杀毒软件，即 Asiainfo Security 和 Trend Micro，供 troubleshooting 分析。

PS：从我们的经验分析，不同安防类软件的 hook 方法可能会导致死锁或者一些想不到的结果。

李琦 Li Qi

神州网信技术有限公司

C&M Information Technologies Co.,Ltd.

服务电话： 4008180055

电子邮箱 Email: liqi@cmgos.com

神州网信
CMIT