张先生 您好:

感谢您的电话接听。

如刚才电话沟通，近期电脑未再次出现蓝屏问题，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：

用户反馈在 V0-H 时出现过蓝屏问题，在升级至 V2020-L 后，再次出现系统蓝屏问题。

问题总结：

用户反馈近期未再次出现蓝屏问题，暂时关闭案例；如后续再次出现蓝屏问题，请上传日志后再次分析。

问题分析：

此 dump 的 bugcheck code 是 0x1a，出现蓝屏的原因是 0x41792，这表示检测到损坏的 PTE。

dump 具体分析如下:

查看 bugcheck 分析情况，显示 0x1a 报错代码，检测到损坏的 PTE。

```
*******************************************************************************
*                                                                             *
*                        Bugcheck Analysis                                    *
*                                                                             *
*******************************************************************************

MEMORY_MANAGEMENT (1a)
    # Any other values for parameter 1 must be individually examined.
Arguments:
Arg1: 0000000000041792, A corrupt PTE has been detected. Parameter 2 contains the address of
      the PTE. Parameters 3/4 contain the low/high parts of the PTE.
Arg2: ffff8000be800090
Arg3: 0001000000000000
Arg4: 0000000000000000

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

从出错的 call stack 中，可以看到在 thread 退出的时候，清理相关内存的操作；此 call stack 中，有 VSApiNt 和 TmXPFlt 组件。

```
7: kd> kn
 # Child-SP          RetAddr           Call Site
00 ffff978b`d298ddc8 fffff807`5f6c1b59 nt!KeBugCheckEx
01 ffff978b`d298ddd0 fffff807`5f54b12e nt!MiDeleteVa+0x171f99
02 ffff978b`d298dee0 fffff807`5f54ac94 nt!MiWalkPageTablesRecursively+0x127e
03 ffff978b`d298dfc0 fffff807`5f54ac94 nt!MiWalkPageTablesRecursively+0xde4
04 ffff978b`d298e0a0 fffff807`5f54ac94 nt!MiWalkPageTablesRecursively+0xde4
05 ffff978b`d298e180 fffff807`5f549b4a nt!MiWalkPageTablesRecursively+0xde4
06 ffff978b`d298e260 fffff807`5f54c3cd nt!MiWalkPageTables+0x1da
07 ffff978b`d298e360 fffff807`5f54cf25 nt!MiDeletePagablePteRange+0x1dd
08 ffff978b`d298e5a0 fffff807`5fa5bd81 nt!MiDeleteVad+0x7c5
09 ffff978b`d298e710 fffff807`5fa5bb7f nt!MiUnmapVad+0x49
0a ffff978b`d298e740 fffff807`5fa5ba29 nt!MiUnmapViewOfSection+0x11f
0b ffff978b`d298e820 fffff807`5fa5b92c nt!NtUnmapViewOfSectionEx+0x99
0c ffff978b`d298e870 fffff807`5f680305 nt!NtUnmapViewOfSection+0xc
0d ffff978b`d298e8a0 fffff807`5f672db0 nt!KiSystemServiceCopyEnd+0x25
0e ffff978b`d298ea38 fffff807`5df883fd nt!KiServiceLinkage
0f ffff978b`d298ea40 fffff807`5dfcb8e1 VSApiNt+0x1883fd
10 ffff978b`d298ea70 fffff807`5dfcf720 VSApiNt+0x1cb8e1
11 ffff978b`d298eb50 fffff807`5dfba13e VSApiNt+0x1cf720
12 ffff978b`d298ebd0 fffff807`5dfbba18 VSApiNt+0x1ba13e
13 ffff978b`d298ec40 fffff807`5df2e0d7 VSApiNt+0x1bba18
14 ffff978b`d298ec80 fffff807`5df04d4d VSApiNt+0x12e0d7
15 ffff978b`d298ecb0 fffff807`5defe47b VSApiNt+0x104d4d
16 ffff978b`d298f280 fffff807`5df2c2ad VSApiNt+0xfe47b
17 ffff978b`d298f370 fffff807`5df2ceaf VSApiNt+0x12c2ad
18 ffff978b`d298f3f0 fffff807`5df2d67d VSApiNt+0x12ceaf
19 ffff978b`d298f460 fffff807`5df2e905 VSApiNt+0x12d67d
1a ffff978b`d298f4e0 fffff807`5df1c28f VSApiNt+0x12e905
1b ffff978b`d298f560 fffff807`5df7eb67 VSApiNt+0x11c28f
1c ffff978b`d298f610 fffff807`5de045ad VSApiNt+0x17eb67
1d ffff978b`d298f650 fffff807`5de0236a VSApiNt+0x45ad
1e ffff978b`d298f6f0 fffff807`5dfbdd40 VSApiNt+0x236a
1f ffff978b`d298f7c0 fffff807`5e896cdc VSApiNt+0x1bdd40
20 ffff978b`d298f850 fffff807`5e898711 TmXPFlt+0x26cdc
21 ffff978b`d298f890 fffff807`5e88015d TmXPFlt+0x28711
22 ffff978b`d298f8e0 fffff807`5e880c44 TmXPFlt+0x1015d
23 ffff978b`d298fa20 fffff807`5e880f68 TmXPFlt+0x10c44
24 ffff978b`d298fae0 fffff807`5f5e4195 TmXPFlt+0x10f68
25 ffff978b`d298fb10 fffff807`5f67651c nt!PspSystemThreadStartup+0x55
26 ffff978b`d298fb60 00000000`00000000 nt!KiStartSystemThread+0x1c
```

查看当前的 PTE 结构有损坏。

```
7: kd> .frame /r 1
01 ffff978b`d298ddd0 fffff807`5f54b12e nt!MiDeleteVa+0x171f99
rax=0000000000000000 rbx=0001000000000000 rcx=000000000000001a
rdx=0000000000041792 rsi=ffff8000be800090 rdi=ffff978bd298e3d0
rip=fffff8075f6c1b59 rsp=ffff978bd298ddd0 rbp=ffff978bd298de79
 r8=ffff8000be800090  r9=0001000000000000 r10=0000000000000000
r11=ffffbe052dc62540 r12=0000017d00012000 r13=0000000000000042
r14=ffff978bd298e480 r15=ffff978bd298e390
iopl=0         nv up ei pl zr na po nc
cs=0010  ss=0018  ds=002b  es=002b  fs=0053  gs=002b             efl=00000246
nt!MiDeleteVa+0x171f99:
fffff807`5f6c1b59 cc              int     3
7: kd> !pte ffff8000be800090
                                           VA 0000017d00012000
PXE at FFFF804020100010    PPE at FFFF804020002FA0    PDE at FFFF8040005F4000    PTE at FFFF8000BE800090
contains 8A0000012F9B3867  contains 0A000002628B4867  contains 1A000002846B5867  contains 0001000000000000
pfn 12f9b3    ---DA--UW-V  pfn 2628b4    ---DA--UWEV  pfn 2846b5    ---DA--UWEV  not valid
                                                                                  Page has been freed
```

查看 VSApiNt 和 TmXPFlt 组件信息

```
7: kd> lmvm VSApiNt
Browse full module list
start             end                 module name
fffff807`5de00000 fffff807`5e0ad000   VSApiNt    (no symbols)
    Loaded symbol image file: VSApiNt.sys
    Image path: \??\C:\Program Files (x86)\Asiainfo Security\OfficeScan Client\VSApiNt.sys
    Image name: VSApiNt.sys
    Browse all global symbols  functions  data
    Timestamp:        Sun Sep 15 21:28:14 2019 (5D7E3C6E)
    CheckSum:         002B4254
    ImageSize:        002AD000
    Translations:     0000.04b0 0000.04e4 0409.04b0 0409.04e4
    Information from resource tables:
7: kd> lmvm TmXPFlt
Browse full module list
start             end                 module name
fffff807`5e870000 fffff807`5e907000   TmXPFlt    (no symbols)
    Loaded symbol image file: TmXPFlt.sys
    Image path: \??\C:\Program Files (x86)\Asiainfo Security\OfficeScan Client\TmXPFlt.sys
    Image name: TmXPFlt.sys
    Browse all global symbols  functions  data
    Timestamp:        Sun Sep 15 21:29:02 2019 (5D7E3C9E)
    CheckSum:         00069722
    ImageSize:        00097000
    Translations:     0000.04b0 0000.04e4 0409.04b0 0409.04e4
    Information from resource tables:
```

VSApiNt 和 TmXPFlt 是亚信安全软件的组件，针对此问题，**建议删除或更新亚信安全软件后，观察是否再次出现蓝屏现象。**

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

发件人: Wei Liang <weiliang@cmgos.com>
发送时间: 2021 年 11 月 30 日 11:19
收件人: 吴毓杰 <win10sup@sdc.icbc.com.cn>
抄送: Wei Liang <weiliang@cmgos.com>
主题: [案例号：CAS-05206-V2V9F5] % |P2|ICBC|系统蓝屏需要协助分析 % 初次响应 CMIT:0001329

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-05206-V2V9F5 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
