许先生 您好:

感谢您的电话接听。

确认您的问题已经解决，我将归档此案例。

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：

工行反馈有生产环境中的设备在登录界面等待一段时间，或者登录到桌面一会后，出现系统卡死的现象，需要协助排查。

问题总结：

通过分析手动触发的 dump，均显示问题与 tmcomm.sys 驱动有关，这是亚信安全的驱动，是这个驱动导致系统无响应。

经过测试，安装新版本的亚信安全软件后，不再出现问题，案例关闭。

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: 2023 年 12 月 12 日 14:36
收件人: ICBC 案例通知 <win10sup@sdc.icbc.com.cn>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>

主题: 回复: [案例号: CAS-10425-X7R4Y3] % |P2|ICBC|工行反馈在输入密码后系统卡死问题 % 初次响应 CMIT:0001721

许先生 您好:

刚刚给您的电话没有接通。

来信是想询问当前案例情况。请您与最终用户确认，安装新版本的亚信安全软件后，是否有再次出现系统卡死的现象。

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 12 月 7 日 17:49
收件人: ICBC 案例通知 <win10sup@sdc.icbc.com.cn>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: [案例号: CAS-10425-X7R4Y3] % |P2|ICBC|工行反馈在输入密码后系统卡死问题 % 初次响应 CMIT:0001721

许先生 您好:

针对此案例，共获取了三个手动触发的 dump，这三个 dump 均显示问题与 tmcomm.sys 驱动有关，这是亚信安全的驱动，目前看到是这个驱动导致系统无响应。

测试建议:

1、先将亚信安全软件临时卸载，测试、观察是否还复现问题。

2、也可以联系三方应用厂商检查驱动情况。

dump 详细分析：

以启动一段时间后死机的 dump 为例：

系统中有个 lock 的 system 线程 ffffb3011ecd8040

```
0: kd> !locks
**** DUMP OF ALL RESOURCE OBJECTS ****
KD: Scanning for held locks....

Resource @ pdc!PdcLock (0xfffff8062e6301a0)    Exclusively owned
    Contention Count = 3
     Threads: ffffb3011ecd8040-01<*>
KD: Scanning for held locks.....................................................
```

等待在 tmbmsrv.exe，与 tmcomm.sys 有关

```
0: kd> !mex.t ffffb3011ecd8040
Process                 Thread                  CID      UserTime KernelTime ContextSwitches Wait Reason    Time State
System (ffffb301118a4040) ffffb3011ecd8040 (E|K|W|R|V) 4.1250          0       31ms            2063 WrLpcReply  11s.375 Waiting

WaitBlockList:
    Object           Type      Other Waiters Info
    ffffb3011ecd8688 Semaphore             0 Limit: 1

Priority:
    Current Base Decrement ForegroundBoost IO Page
    12      12   0         0               0  5

LPC Msg          ServerProcess                 ServerThread
ffffda881bf0abc0 TMBMSRV.exe(ffffb301206b3080) Message Queued

 # Child-SP         Return           Call Site
 0 ffffad8231945c60 fffff80618a35807 nt!KiSwapContext+0x76
 1 ffffad8231945da0 fffff80618a35379 nt!KiSwapThread+0x297
 2 ffffad8231945e60 fffff80618a34100 nt!KiCommitThreadWait+0x549
 3 ffffad8231945f00 fffff80618aa9482 nt!KeWaitForSingleObject+0x520
 4 ffffad8231945fd0 fffff80619018d56 nt!AlpcpSignalAndWait+0x222
 5 ffffad8231946070 fffff80619018865 nt!AlpcpReceiveSynchronousReply+0x56
 6 ffffad82319460d0 fffff806190b6b8e nt!AlpcpProcessSynchronousRequest+0x3a5
 7 ffffad82319461e0 fffff806190b6ade nt!LpcpRequestWaitReplyPort+0x86
 8 ffffad8231946240 fffff80618be14f5 nt!NtRequestWaitReplyPort+0x6e
 9 ffffad8231946280 fffff80618bd2da0 nt!KiSystemServiceCopyEnd+0x25
 a ffffad8231946418 fffff80630a0a665 nt!KiServiceLinkage
 b ffffad8231946420 fffff80630a0b239 tmcomm!KmSetCommPortAPIs+0x7f1
 c ffffad8231946950 fffff80630a09e36 tmcomm!InitKmLPC+0x23d
 d ffffad82319469d0 fffff80631a7b487 tmcomm!KmCallUmEx+0x26
 e ffffad8231946a00 fffff80631a7dee0 tmactmon+0xb487
 f ffffad8231946aa0 fffff80631a7dcd1 tmactmon+0xdee0
10 ffffad8231946b10 fffff80631a5170e tmactmon+0xdcd1
```

查看另一个 lock 的线程 ffffb301206a7080

```
Resource @ 0xffffb3011b90b910    Exclusively owned
    Contention Count = 216767
    NumberOfSharedWaiters = 3
    NumberOfExclusiveWaiters = 18
     Threads: ffffb301206a7080-01<*> ffffb3011db9c080-01    ffffb3011dd82080-01    ffffb301221d40c0-01

     Threads Waiting On Exclusive Access:
             ffffb3011ded7480       ffffb3011da146c0       ffffb30122858080       ffffb3011e482040
             ffffb301220ea0c0       ffffb301207020c0       ffffb30121b57080       ffffb3012210e080
             ffffb30121e875c0       ffffb3012127c080       ffffb301211d1080       ffffb30122071080
             ffffb301206a8080       ffffb301209a4080       ffffb30121e59040       ffffb3011dbf7080
             ffffb30121fa2080       ffffb3011d943080
KD: Scanning for held locks.
```

该线程是在处理 dxgmms2 相关的事情并等在 kernel 的组件上。 通过 callstack 搜索。另外一个处理该请求的线程（ffffb3011c5d4680）卡在了 tmcomm.sys 这个驱动上。

```
0: kd> !mex.t ffffb301206a7080
Process                 AttachedProcess           Thread                    CID      TEB              UserTime KernelTime ContextSwitches
dwm.exe (ffffb3011db75080) csrss.exe (ffffb3011da18140) ffffb301206a7080 (E|K|W|R|V) 6cc.37e8  000000eff8936000        0          0             10
WaitBlockList:
    Object           Type                Other Waiters
    ffffb30121cf3760 SynchronizationEvent            0
Priority:
    Current Base Decrement ForegroundBoost IO Page
    15      13   0         16              0  5
 # Child-SP         Return           Call Site
 0 ffffad8234525a00 fffff80618a35807 nt!KiSwapContext+0x76
 1 ffffad8234525b40 fffff80618a35379 nt!KiSwapThread+0x297
 2 ffffad8234525c00 fffff80618a34100 nt!KiCommitThreadWait+0x549
 3 ffffad8234525ca0 fffff806314847f2 nt!KeWaitForSingleObject+0x520
 4 ffffad8234525d70 fffff8063146e27a dxgmms2!VIDMM_GLOBAL::WaitForFences+0x292
 5 ffffad8234525e90 fffff8063146debb dxgmms2!VIDMM_GLOBAL::QueueDeferredCommand+0x1e6
 6 ffffad8234525f20 fffff8063146dc4d dxgmms2!VIDMM_GLOBAL::VidMmMapGpuVirtualAddressInternal+0x22f
 7 ffffad8234526080 fffff80631411b99 dxgmms2!VIDMM_GLOBAL::VidMmMapGpuVirtualAddress+0xa5
 8 ffffad82345260d0 fffff8061a629b7d dxgmms2!VidMmMapGpuVirtualAddress+0x19
 9 ffffad8234526110 fffff8061a6f089f dxgkrnl!VIDMM_EXPORT::VidMmMapGpuVirtualAddress+0x41
 a ffffad8234526160 fffff8061a7032bc dxgkrnl!DXGDEVICE::CreateAllocation+0x266f
 b ffffad82345264d0 fffff8061a703acb dxgkrnl!DXGDEVICE::CreateStandardAllocation+0x2fc
 c ffffad8234526820 fffff4c86b7f98e4 dxgkrnl!DxgkCddCreateAllocation+0x24b
 d ffffad8234526b70 fffff4c86b7f9724 cdd!CDDPDEV::CreateAllocation+0x158
 e ffffad8234526cd0 fffff4c86b7f7b85 cdd!CddBitmapHw::RecreateDeviceAllocations+0xc4
 f ffffad8234526d60 fffff4c86b7f8b3d cdd!CddBitmapHw::InitBitmap+0x95
```

```
0: kd> !mex.t ffffb3011c5d4680
Process                 Thread                    CID      UserTime KernelTime ContextSwitches Wait Reason      Time State
System (ffffb301118a4040) ffffb3011c5d4680 (E|K|W|R|V) 4.3ec           0       94ms            1909 WrLpcReply  2m:47.468 Waiting
WaitBlockList:
    Object           Type      Other Waiters Info
    ffffb3011c5d4cc8 Semaphore             0 Limit: 1
Priority:
    Current Base Decrement ForegroundBoost IO Page
    15      15   0         0               0  5
LPC Msg          ServerProcess                ServerThread
ffffda881cc24c60 TMBMSRV.exe(ffffb301206b3080) Message Queued
 # Child-SP         Return           Call Site
 0 ffffad822f9adbe0 fffff80618a35807 nt!KiSwapContext+0x76
 1 ffffad822f9add20 fffff80618a35379 nt!KiSwapThread+0x297
 2 ffffad822f9adde0 fffff80618a34100 nt!KiCommitThreadWait+0x549
 3 ffffad822f9ade80 fffff80618aa9482 nt!KeWaitForSingleObject+0x520
 4 ffffad822f9adf50 fffff80619018d56 nt!AlpcpSignalAndWait+0x222
 5 ffffad822f9adff0 fffff80619018865 nt!AlpcpReceiveSynchronousReply+0x56
 6 ffffad822f9ae050 fffff806190b6b8e nt!AlpcpProcessSynchronousRequest+0x3a5
 7 ffffad822f9ae160 fffff806190b6ade nt!LpcpRequestWaitReplyPort+0x86
 8 ffffad822f9ae1c0 fffff80618be14f5 nt!NtRequestWaitReplyPort+0x6e
 9 ffffad822f9ae200 fffff80618bd2da0 nt!KiSystemServiceCopyEnd+0x25
 a ffffad822f9ae398 fffff80630a0a665 nt!KiServiceLinkage
 b ffffad822f9ae3a0 fffff80630a0b239 tmcomm!KmSetCommPortAPIs+0x7f1
 c ffffad822f9ae8d0 fffff80630a09e36 tmcomm!InitKmLPC+0x23d
 d ffffad822f9ae950 fffff80631a7b487 tmcomm!KmCallUmEx+0x26
 e ffffad822f9ae980 fffff80631a7b192 tmactmon+0xb487
 f ffffad822f9aea20 fffff80631a7c59b tmactmon+0xb192
10 ffffad822f9aeb60 fffff80631a7c33a tmactmon+0xc59b
11 ffffad822f9aec10 fffff80631a5b473 tmactmon+0xc33a
12 ffffad822f9aec40 fffff80631a5a906 tmevtmgr!TMEvtCommunicateRoutine+0x2503
13 ffffad822f9aec70 fffff8061901bc4a tmevtmgr!TMEvtCommunicateRoutine+0x1996
14 ffffad822f9aed40 fffff80618fee39e nt!ObpCallPreOperationCallbacks+0xfa
15 ffffad822f9aedc0 fffff80619063ad4 nt!ObpCreateHandle+0xd4e
16 ffffad822f9af000 fffff80619063ee9 nt!ObOpenObjectByPointer+0x184
17 ffffad822f9af280 fffff80619062e93 nt!PsOpenProcess+0x289
```

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: 2023 年 12 月 6 日 16:51
收件人: ICBC 案例通知 <win10sup@sdc.icbc.com.cn>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: [案例号: CAS-10425-X7R4Y3] % |P2|ICBC|工行反馈在输入密码后系统卡死问题 % 初次响应 CMIT:0001721

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:

工行反馈有生产环境中的设备在登录界面等待一段时间，或者登录到桌面一会后，出现系统卡死的现象，需要协助排查。

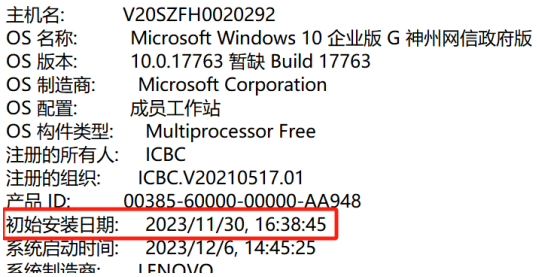
问题范围:

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。

当前收集的系统日志显示系统是 2023 年 11 月 30 日安装的系统，查看相关系统日志未发现可能的问题点。

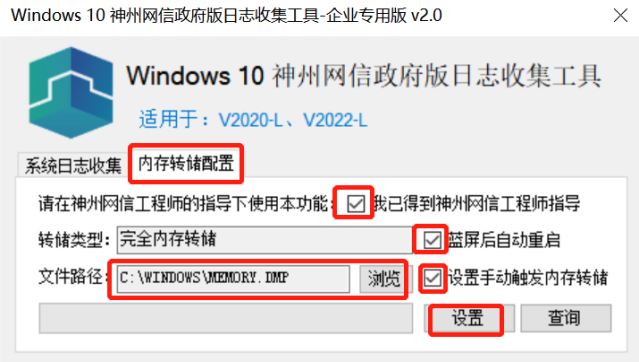


请您确认以下情况并进行相关日志收集：

1）出现这个问题时是否有做过哪些应用安装或升级操作？升级的应用是否可以卸载或回退？

2）测试断开网络后是否可以正常进入系统不发生卡死问题？

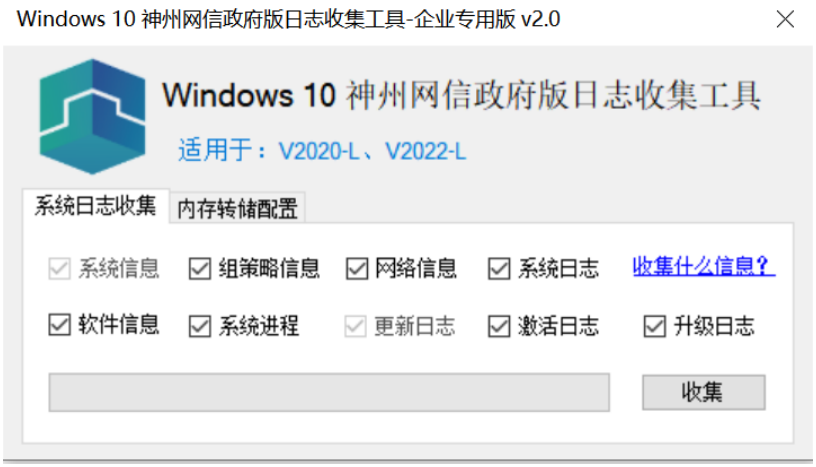
3）在出现卡死问题的设备上双击运行 CMGELogCollectorV2.exe，在日志收集工具窗口点击**“内存转储配置”**，勾选**“我已得到神州网信工程师指导”**、**“蓝屏后自动重启”**和**“设置手动触发内存转储”**，并设置文件路径，点击**“设置”**后完成手动触发蓝屏配置，需要**重启计算机生效。**



4）在故障设备上**复现系统卡死问题，此时在系统卡死状态下，**直接通过键盘组合键**左 shift + 右 shift 按住不放，连按两次波浪号键“~”（Esc 下方）**，手动触发蓝屏，生成 C:\Windows\memory.dmp 文件。

5）确认 C:\Windows\memory.dmp 是最新生成的，将 memory.dmp 文件**压缩后**通过 **CDUC** 上传。

6）再次运行 **CMGELogCollectorV2.exe**，勾选**所有选项**，点击收集获取对应的系统日志，将生成的日志压缩包通过 CDUC 上传。



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 <weiliang@cmgos.com>
发送时间: 2023 年 12 月 6 日 15:11
收件人: ICBC 案例通知 <win10sup@sdc.icbc.com.cn>
抄送: Wei Liang <weiliang@cmgos.com>
主题: [案例号：CAS-10425-X7R4Y3] % |P2|ICBC|工行反馈在输入密码后系统卡死问题 % 初次响应 CMIT:0001721

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-10425-X7R4Y3 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
