侯先生 您好:

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：

用户反馈系统安装应用软件后运行一段时间后蓝屏，重启后反复蓝屏无法进入系统，需要协助排查。

问题总结：

确认是应用所带的 hardlock 驱动导致蓝屏问题，禁用 hardlock 驱动后系统可以正常运行。

日志分析：

memory.dmp 文件显示是 hardlock.sys 驱动导致的蓝屏问题，其访问了 0 地址导致蓝屏。

```
Priority 13 BasePriority 12 PriorityDecrement 0 IoPriority 2 PagePriority 5
Child-SP          RetAddr           : Args to Child                                                   : Call Site
ffffc283`5b1852b8 fffff802`3e011b7a : 00000000`0000007e ffffffff`80000003 fffff802`3df408b3 ffffc283`5b1862b8 : nt!KeBugCheckEx
ffffc283`5b1852c0 fffff802`3dfce32f : fffff802`00000003 fffff802`3dccdd10 ffffc283`5b181000 ffffc283`5b188000 : nt!PspSystemThreadStartup$filt$0+0x44
ffffc283`5b185300 fffff802`3e001e8f : fffff802`3dccdd10 ffffc283`5b1858e0 fffff802`3dfce290 00000000`00000000 : nt!_C_specific_handler+0x9f
ffffc283`5b185370 fffff802`3de77a77 : ffffc283`5b1858e0 00000000`00000000 ffffc283`5b187b10 fffff802`3de71d25 : nt!RtlpExecuteHandlerForException+0xf
ffffc283`5b1853a0 fffff802`3de76676 : ffffc283`5b1862b8 ffffc283`5b185ff0 ffffc283`5b1862b8 00000000`00000000 : nt!RtlDispatchException+0x297
ffffc283`5b185ac0 fffff802`3e00b0ac : ffffc283`5b187190 00007fff`ffffffff ffffc283`5b186240 ffffc283`5b186746 : nt!KiDispatchException+0x186
ffffc283`5b186180 fffff802`3e004a16 : 00000000`00000000 00000000`00000000 00000000`00040293 fffff802`3de3546b : nt!KiExceptionDispatch+0x12c
ffffc283`5b186360 fffff802`3df408b4 : ffffc283`5b186558 ffffc283`5b186598 00000000`00000000 ffffc283`5b186600 : nt!KiBreakpointTrap+0x316 (TrapFrame @ ffffc283`5b18
ffffc283`5b1864f0 fffff802`3dfce2cb : fffff802`3de71d25 fffff802`3dccdd10 00000000`00000000 00000000`00000000 : nt!KeCheckStackAndTargetAddress+0x54
ffffc283`5b186520 fffff802`3e001e8f : fffff802`3dccdd10 ffffc283`5b186b00 fffff802`3dfce290 00000000`00000000 : nt!_C_specific_handler+0x3b
ffffc283`5b186590 fffff802`3de77a77 : ffffc283`5b186b00 00000000`00000000 ffffc283`5b187b10 fffff802`3de71d25 : nt!RtlpExecuteHandlerForException+0xf
ffffc283`5b1865c0 fffff802`3de76676 : ffffc283`5b1874d8 ffffc283`5b187210 ffffc283`5b1874d8 ffffca08`15ff4e20 : nt!RtlDispatchException+0x297
ffffc283`5b186ce0 fffff802`3e00b0ac : 00000000`00001000 ffffc283`5b187580 ffff8000`00000000 00000000`00000000 : nt!KiDispatchException+0x186
ffffc283`5b1873a0 fffff802`3e007243 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000090 : nt!KiExceptionDispatch+0x12c
ffffc283`5b187580 00000000`00000000 : fffff802`bfe9c197 ffffdc00`f176fed0 ffff817c`011eeab8 ffff8140`be008f70 : nt!KiPageFault+0x443 (TrapFrame @ ffffc283`5b187580)

1: kd> .trap ffffc283`5b187580
NOTE: The trap frame does not contain all registers.
Some register values may be zeroed or incorrect.
rax=fffff802bfe94260 rbx=0000000000000000 rcx=fffff802bfe942e0
rdx=0000000000000001 rsi=0000000000000000 rdi=0000000000000000
rip=0000000000000000 rsp=ffffc2835b187718 rbp=ffffc2835b187960
 r8=ffffc2835b187701  r9=0000000000000100 r10=fffff802bfe9e1de
r11=0000000000000000 r12=0000000000000000 r13=0000000000000000
r14=0000000000000000 r15=0000000000000000
iopl=0         nv up ei pl zr na po nc
00000000`00000000 ??              ???
1: kd> kvn
  *** Stack trace for last set context - .thread/.cxr resets it
 # Child-SP          RetAddr           : Args to Child                                                   : Call Site
00 ffffc283`5b187718 fffff802`bfe9c197 : ffffdc00`f176fed0 ffff817c`011eeab8 ffff8140`be008f70 fffff802`3dd57000 : 0x0
01 ffffc283`5b187720 fffff802`3e361a2c : ffffca08`15ff4e20 ffffca08`1b3ff000 ffffca08`1b3ff000 00000000`00000000 : hardlock+0x4c197
02 ffffc283`5b187800 fffff802`3e32d1bd : 00000000`00000012 00000000`00000000 00000000`00000000 00000000`00001000 : nt!PnpCallDriverEntry+0x4c
03 ffffc283`5b187860 fffff802`3e3724c7 : 00000000`00000000 00000000`00000000 fffff802`3e925440 ffffca07`f9cd5ec0 : nt!IopLoadDriver+0x4e5
04 ffffc283`5b187a30 fffff802`3de52b65 : ffffca08`00000000 ffffffff`80002838 ffffca08`15512040 fffff802`00000000 : nt!IopLoadUnloadDriver+0x57
05 ffffc283`5b187a70 fffff802`3de71d25 : ffffca08`15512040 00000000`00000080 ffffca07`f9cc8100 000fa4ef`bd9bbfff : nt!ExpWorkerThread+0x105
06 ffffc283`5b187b10 fffff802`3e000628 : ffff8181`31a79180 ffffca08`15512040 fffff802`3de71cd0 00000000`00000000 : nt!PspSystemThreadStartup+0x55
07 ffffc283`5b187b60 00000000`00000000 : ffffc283`5b188000 ffffc283`5b181000 00000000`00000000 00000000`00000000 : nt!KiStartSystemThread+0x28
```

查看 hardlock 驱动情况:

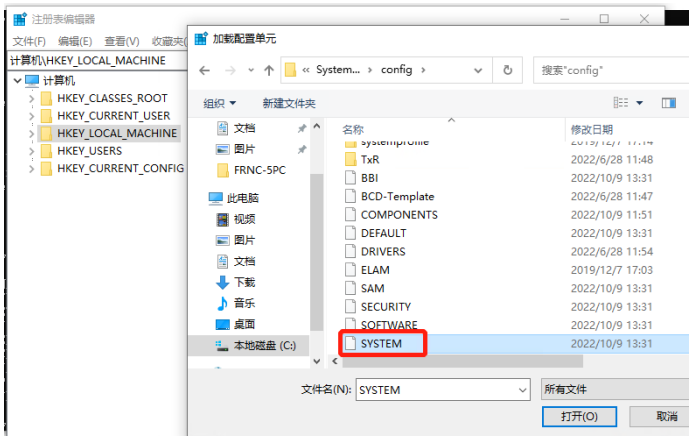
```
1: kd> lmvm hardlock
Browse full module list
start             end                 module name
fffff802`bfe50000 fffff802`bfe9f600   hardlock   (no symbols)
    Loaded symbol image file: hardlock.sys
    Image path: \??\C:\Windows\system32\drivers\hardlock.sys
    Image name: hardlock.sys
    Browse all global symbols  functions  data
    Timestamp:        Tue Mar 24 01:19:26 2015 (55104B1E)
    CheckSum:         000396DA
    ImageSize:        0004F600
    File version:     3.87.51858.1
    Product version:  3.87.51858.1
    File flags:       8 (Mask 3F) Private
    File OS:          40004 NT Win32
    File type:        3.7 Driver
    File date:        00000000.00000000
    Translations:     0409.04b0
    Information from resource tables:
        CompanyName:      SafeNet Inc.
        ProductName:      Sentinel Hardlock Device Driver for Windows x64
        InternalName:     hardlock.sys
        OriginalFilename: hardlock.sys
        ProductVersion:   3.87
        FileVersion:      3.87
        FileDescription:  Sentinel Hardlock Device Driver for Windows x64
        LegalCopyright:   (c) 2015 SafeNet, Inc. All rights reserved.
```

通过以下操作修改注册表，禁止加载此驱动。

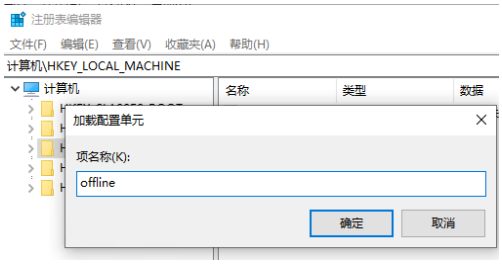
1）启动到 PE 运行环境

2）打开注册表编辑器，选中“HKET_LOCAL_MACHINE”，选择“文件”-“加载配置单元”

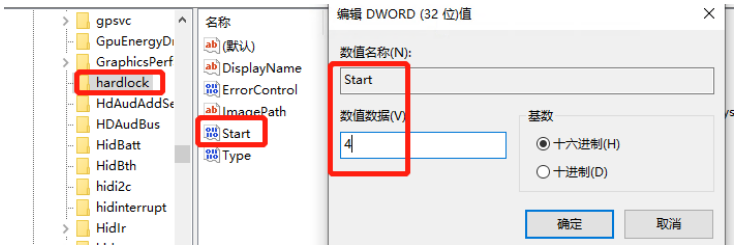
3）在打开的窗口中选择 C:\Windows\system32\config\system



4）为加载的项名称取名为“offline”

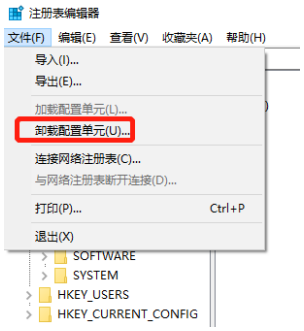


5）展开 HKEY_LOCAL_MACHINE\offline\ControlSer001\Services\hardlock\



修改右边的 Start 键值为 4。

6）选中 offline，选择“文件”-“卸载配置单元”



7）**重新启动验证是否可以正常进入系统。**

也可以在安装应用后不启动应用，先禁用 hardlock 驱动并重启系统后，再运行应用。

打开注册表编辑器，定位到：

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\hardlock，修改 Start 键值为 4，重启计算机生效。

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
发送时间: 2022 年 10 月 9 日 14:48
收件人: 'wyx486' <wyx486@126.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: 回复: Re:回复: [案例号: CAS-07286-Q6F8W5]％ 中国石油天然气集团有限公司用户反馈系统蓝屏问题 ％初次响应 CMIT:0001353

侯先生 您好:

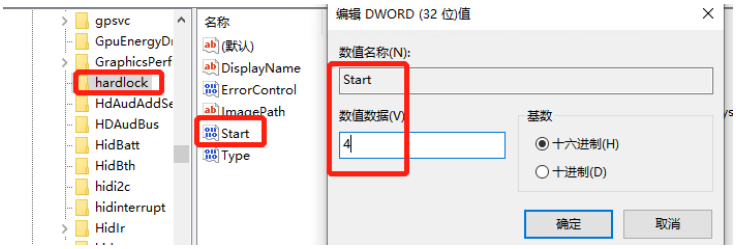
感谢您的电话接听。

如电话中所说，您可以按照以下操作**先禁用 hardlock.sys 驱动，并重启计算机，**再运行您安装的应用。

1）正常安装应用完成后，先**不运行**应用。

2）运行 regedit，打开注册表编辑器，定位到:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\hardlock



修改右边的 Start 键值为 4。

3）重启计算机禁用 hardlock 驱动，再运行您安装的应用。

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: wyx486 <wyx486@126.com>
发送时间: 2022 年 10 月 9 日 14:32
收件人: Wei Liang <weiliang@cmgos.com>
主题: Re:回复: [案例号: CAS-07286-Q6F8W5] % 中国石油天然气集团有限公司用户反馈系统蓝屏问题 % 初次响应 CMIT:0001353

加载配置单元显示，找不到 ssystem32

在 2022-10-09 14:01:46，"Wei Liang" <weiliang@cmgos.com> 写道：

> 侯先生 您好:
>
> 感谢您的电话接听。
>
> 查看您提供的 memory.dmp 文件，显示是 hardlock.sys 驱动导致的蓝屏问题，其访问了 0 地址导致蓝屏。

```
Priority 13 BasePriority 12 PriorityDecrement 0 IoPriority 2 PagePriority 5
Child-SP          RetAddr           : Args to Child                                                   : Call Site
ffffc283`5b1852b8 fffff802`3e011b7a : 00000000`0000007e ffffffff`80000003 fffff802`3df408b3 ffffc283`5b1862b8 : nt!KeBugCheckEx
ffffc283`5b1852c0 fffff802`3dfce32f : fffff802`00000003 fffff802`3dccdd10 ffffc283`5b181000 ffffc283`5b188000 : nt!PspSystemThreadStartup$filt$0+0x44
ffffc283`5b185300 fffff802`3e001e8f : fffff802`3dccdd10 ffffc283`5b1858e0 fffff802`3dfce290 00000000`00000000 : nt!_C_specific_handler+0x9f
ffffc283`5b185370 fffff802`3de77a77 : ffffc283`5b1858e0 00000000`00000000 ffffc283`5b187b10 fffff802`3de71d25 : nt!RtlpExecuteHandlerForException+0xf
ffffc283`5b1853a0 fffff802`3de76676 : ffffc283`5b1862b8 ffffc283`5b185ff0 ffffc283`5b1862b8 00000000`00000000 : nt!RtlDispatchException+0x297
ffffc283`5b185ac0 fffff802`3e00b0ac : ffffc283`5b187190 00007fff`fffeffff ffffc283`5b186240 ffffc283`5b186746 : nt!KiDispatchException+0x186
ffffc283`5b186180 fffff802`3e004a16 : 00000000`00000000 00000000`00000000 00000000`00040293 fffff802`3de3546b : nt!KiExceptionDispatch+0x12c
ffffc283`5b186360 fffff802`3df408b4 : ffffc283`5b186558 ffffc283`5b186598 00000000`00000000 ffffc283`5b186600 : nt!KiBreakpointTrap+0x316 (TrapFrame @ ffffc283`5b
ffffc283`5b1864f0 fffff802`3dfce2cb : fffff802`3de71d25 fffff802`3dccdd10 00000000`00000000 00000000`00000000 : nt!KeCheckStackAndTargetAddress+0x54
ffffc283`5b186520 fffff802`3e001e8f : fffff802`3dccdd10 ffffc283`5b186b00 fffff802`3dfce290 00000000`00000000 : nt!_C_specific_handler+0x3b
ffffc283`5b186590 fffff802`3de77a77 : ffffc283`5b186b00 00000000`00000000 ffffc283`5b187b10 fffff802`3de71d25 : nt!RtlpExecuteHandlerForException+0xf
ffffc283`5b1865c0 fffff802`3de76676 : ffffc283`5b1874d8 ffffc283`5b187210 ffffc283`5b1874d8 ffffca08`15ff4e20 : nt!RtlDispatchException+0x297
ffffc283`5b186ce0 fffff802`3e00b0ac : 00000000`00001000 ffffc283`5b187580 ffff8000`00000000 00000000`00000000 : nt!KiDispatchException+0x186
ffffc283`5b1873a0 fffff802`3e007243 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000090 : nt!KiExceptionDispatch+0x12c
ffffc283`5b187580 00000000`00000000 : fffff802`bfe9c197 ffffdc00`f176fed0 ffff817c`011eeab8 ffff8140`be008f70 : nt!KiPageFault+0x443 (TrapFrame @ ffffc283`5b18758

1: kd> .trap ffffc283`5b187580
NOTE: The trap frame does not contain all registers.
Some register values may be zeroed or incorrect.
rax=fffff802bfe94260 rbx=0000000000000000 rcx=fffff802bfe942e0
rdx=0000000000000001 rsi=0000000000000000 rdi=0000000000000000
rip=0000000000000000 rsp=ffffc2835b187718 rbp=ffffc2835b187960
 r8=ffffc2835b187701  r9=0000000000000100 r10=fffff802bfe9elde
r11=0000000000000000 r12=0000000000000000 r13=0000000000000000
r14=0000000000000000 r15=0000000000000000
iopl=0         nv up ei pl zr na po nc
00000000`00000000 ??              ???
1: kd> kvn
  *** Stack trace for last set context - .thread/.cxr resets it
 # Child-SP          RetAddr           : Args to Child                                                   : Call Site
00 ffffc283`5b187718 fffff802`bfe9c197 : ffffdc00`f176fed0 ffff817c`011eeab8 ffff8140`be008f70 fffff802`3dd57000 : 0x0
01 ffffc283`5b187720 fffff802`3e361a2c : ffffca08`15ff4e20 ffffca08`1b3ff000 ffffca08`1b3ff000 00000000`00000000 : hardlock+0x4c197
02 ffffc283`5b187800 fffff802`3e32d1bd : 00000000`00000012 00000000`00000000 00000000`00000000 00000000`00001000 : nt!PnpCallDriverEntry+0x4c
03 ffffc283`5b187860 fffff802`3e3724c7 : 00000000`00000000 00000000`00000000 fffff802`3e925440 ffffca07`f9cd5ec0 : nt!IopLoadDriver+0x4e5
04 ffffc283`5b187a30 fffff802`3de52b65 : ffffca08`00000000 ffffffff`80002838 ffffca08`15512040 fffff802`00000000 : nt!IopLoadUnloadDriver+0x57
05 ffffc283`5b187a70 fffff802`3de71d25 : ffffca08`15512040 00000000`00000080 ffffca07`f9cc8100 000fa4ef`bd9bbfff : nt!ExpWorkerThread+0x105
06 ffffc283`5b187b10 fffff802`3e000628 : ffff8181`31a79180 ffffca08`15512040 fffff802`3de71cd0 00000000`00000000 : nt!PspSystemThreadStartup+0x55
07 ffffc283`5b187b60 00000000`00000000 : ffffc283`5b188000 ffffc283`5b181000 00000000`00000000 00000000`00000000 : nt!KiStartSystemThread+0x28
```

查看 hardlock 驱动情况：

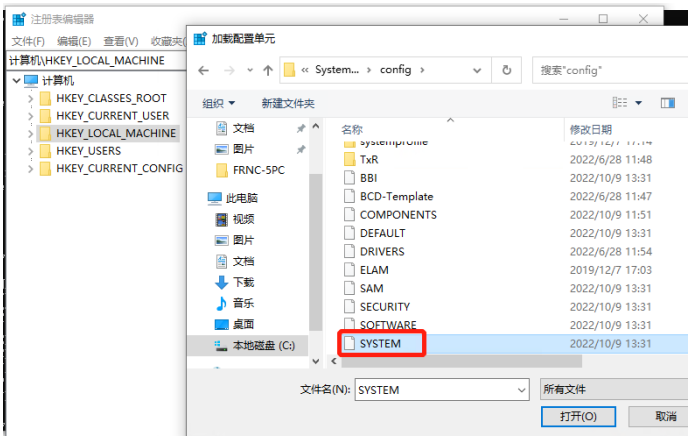
```
1: kd> lmvm hardlock
Browse full module list
start             end                 module name
fffff802`bfe50000 fffff802`bfe9f600   hardlock   (no symbols)
    Loaded symbol image file: hardlock.sys
    Image path: \??\C:\Windows\system32\drivers\hardlock.sys
    Image name: hardlock.sys
    Browse all global symbols  functions  data
    Timestamp:        Tue Mar 24 01:19:26 2015 (55104B1E)
    CheckSum:         000390DA
    ImageSize:        0004F600
    File version:     3.87.51858.1
    Product version:  3.87.51858.1
    File flags:       8 (Mask 3F) Private
    File OS:          40004 NT Win32
    File type:        3.7 Driver
    File date:        00000000.00000000
    Translations:     0409.04b0
    Information from resource tables:
        CompanyName:      SafeNet Inc.
        ProductName:      Sentinel Hardlock Device Driver for Windows x64
        InternalName:     hardlock.sys
        OriginalFilename: hardlock.sys
        ProductVersion:   3.87
        FileVersion:      3.87
        FileDescription:  Sentinel Hardlock Device Driver for Windows x64
        LegalCopyright:   (c) 2015 SafeNet, Inc. All rights reserved.
```

您可以按照以下操作修改注册表，禁止加载此驱动。

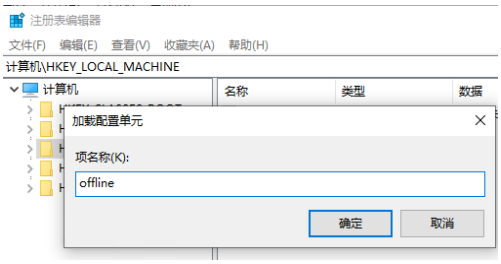
1）启动到 PE 运行环境

2）打开注册表编辑器，选中“HKET_LOCAL_MACHINE”，选择“文件”-“加载配置单元”

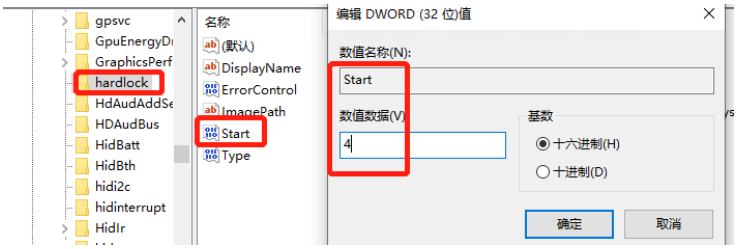
3）在打开的窗口中选择 C:\Windows\system32\config\system



4）为加载的项名称取名为“offline”



5）展开 HKEY_LOCAL_MACHINE\offline\ControlSer001\Services\hardlock\



修改右边的 Start 键值为 4。

6）选中 offline，选择“文件”-“卸载配置单元”

7）**重新启动验证是否可以正常进入系统。**

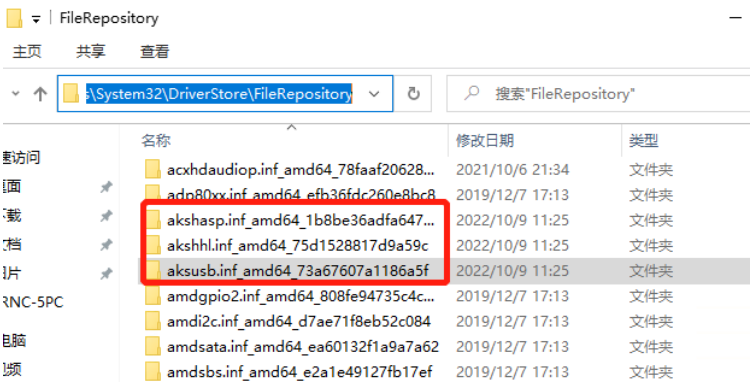
如果禁止此驱动还是蓝屏，可以在 PE 中完全删除对应的驱动文件(如图所示)，再验证系统是否正常启动。

C:\Windows\system32\drivers\hardlock.sys

C:\Windows\system32\DriverStore\FileRepository\akshasp.inf_xxx

C:\Windows\system32\DriverStore\FileRepository\akshhl.inf_xxx

C:\Windows\system32\DriverStore\FileRepository\aksusb.inf_xxx



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: 2022 年 10 月 9 日 10:56
收件人: 侯先生 <wyx486@126.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: 回复: [案例号：CAS-07286-Q6F8W5]％ 中国石油天然气集团有限公司用户反馈系统蓝屏问题 ％初次响应 CMIT:0001353

侯先生 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:

用户反馈系统安装应用软件后运行一段时间后蓝屏，重启后反复蓝屏无法进入系统，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。

请您按照以下方法帮忙收集相关系统日志进行分析。

1）**使用 PE 启动后，复制 C:\Windows\MEMORY.dmp 文件、C:\Windows\minidump 目录和 C:\Windows\system32\winevt\Logs 目录**，将这些文件和文件夹压缩后通过 CDUC 上传。

2）请提供您安装的软件 frnc-5 给我们，尝试复现问题进行排查。

日志上传方法：

您可以登陆 https://cduc.cmgos.com，通过数据上传系统上传您所收集的日志信息。

用户名：jinzhou

密码：jinzhou

注意：添加文件，点击上传后，跳转到新的页面点击保存。

==========

在向 CMIT 提供日志和数据前，请阅读并接受邮件下方隐私声明。

隐私声明

为向您提供本产品的相关技术支持及相关服务，您需要在同意本声明的前提下向神州网信提供为解决系统故障必要的数据和信息，包括但不限于与您相关的个人数据和隐私信息。通常情况下，我们仅需要如下数据以使我们的服务能够更好地满足您的需求：内存转储文件、注册表信息、组策略信息、事件日志、安装应用列表、驱动信息、网络日志或系统补丁等。

神州网信承诺将采取商业上可行及必要措施保护用户提供给神州网信的数据和信息，且仅在解决问题过程中使用。

神州网信保证不对外公开或向第三方提供、公开或共享您提供的数据和信息。

在以下情况下，神州网信对您的数据和信息的披露将不视为违约，具体包括:

(1) 神州网信已获得您的明确授权;

(2) 根据适用法律的要求，神州网信负有披露义务的;

(3) 司法机关或行政机关基于法定程序要求神州网信提供的;

(4) 为维护社会公共利益及神州网信合法权益，在合理范围内进行披露的。

(5) 为了解决您的系统故障问题，神州网信可能会与神州网信的分包商披露您提供的数据和信息。在此情况下，第三方会承担与神州网信同等的隐私保护责任的，神州网信会在合理范围内对您的信息进行披露。

如果您欲提供的数据和信息中包含对您重要的保密信息以及商业秘密，在您向神州网信提供上述数据和信息前，务必对上述数据和信息进行脱敏处理，否则请不要提供该信息给神州网信。作为一家商业软件公司，神州网信在商业可行的前提下，已为用户的数据和信息保护做了极大的努力，但是仍然不能保证现有的安全技术措施使您的数据和信息等不受任何形式的损失。您对上述情况充分知情，且不会因此追究神州网信的法律责任。

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: 2022 年 10 月 9 日 10:19
收件人: 侯先生 <wyx486@126.com>
抄送: Wei Liang <weiliang@cmgos.com>
主题: [案例号：CAS-07286-Q6F8W5] % 中国石油天然气集团有限公司用户反馈系统蓝屏问题 % 初次响应 CMIT:0001353

侯先生 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-07286-Q6F8W5 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