危工程师
给您发了抓包 您给分析谢谢

在 2024-12-12 16:18:39，"王麦熟" <w13731242724@163.com> 写道：

> 您给联系了吗
>
> ---- 回复的原邮件 ----
>
> | | |
> |---|---|
> | 发件人 | Wei Liang<weiliang@cmgos.com> |
> | 发送日期 | 2024 年 09 月 05 日 17:33 |
> | 收件人 | 王麦熟 <w13731242724@163.com> |
> | 抄送人 | PR_Case_Notification <pr_case_notification@cmgos.com> |
> | 主题 | 回复：[案例号：CAS-11760-F7B5H0] % 国网-国网国际发展有限公司用户反馈电脑关机时出现蓝屏的问题 % 初次响应 CMIT：0001575 |
>
> 王先生 您好:
>
> 如电话中所说，在问题设备上的 360 模块的地址为 **C:\Program Files (x86)\360\360safe\safemon\seccscan\Packet.dll**。从对应路径上判断，这个 360 模块名称**可能为 seccscan**。
>
> 可以请 360 人员确认这个模块功能及配置。
>
> 如果针对当前案件需要我们协助，可以通过邮件联系我们，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: 王麦熟 <w13731242724@163.com>
发送时间: 2024 年 9 月 5 日 17:04
收件人: Wei Liang <weiliang@cmgos.com>
主题: Re:回复: Re:回复: Re:回复: Re:回复: 回复： [案例号: CAS-11760-F7B5H0] % 国网-国网国际发展有限公司用户反馈电脑关机时出现蓝屏的问题 % 初次响应 CMIT: 0001575

你好

危亮工程师 我把你发的截图和压缩包发给 360，360 说没有找到你发的截图路径， 我的意思我这有 360 人员的邮箱，你能给他联系一下吗 mashengyuan@360.cn

在 2024-09-04 15:38:10，"Wei Liang" <weiliang@cmgos.com> 写道：

> 王先生 您好:
>
> 来信是想咨询当前案例进展情况。
>
> 如果针对当前案件需要我们协助，可以通过邮件联系我们，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: 2024 年 9 月 2 日 15:19
收件人: '王麦熟' <w13731242724@163.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: 回复: Re:回复: Re:回复: Re:回复: 回复：[案例号: CAS-11760-F7B5H0] % 国网-国网国际发展有限公司用户反馈电脑关机时出现蓝屏的问题 % 初次响应 CMIT: 0001575

王先生 您好:

感谢您的电话接听。

我在本地测试安装 npcap 时，提示有其他进程占用 npf 驱动时，点击“确定”后，npcap 后续按照正常的流程安装成功，且 **C:\Windows\system32\drivers\npf.sys** 驱动被删除。

您也可以按照 npcap 的弹窗提示，在“任务管理器”中结束对应的进程后，再点击“确定”按钮，完成 npcap 的安装。

如果针对当前案件需要我们协助，可以通过邮件联系我们，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: 2024 年 8 月 29 日 15:24
收件人: '王麦熟' <w13731242724@163.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: 回复: Re:回复: Re:回复: Re:回复: 回复：[案例号: CAS-11760-F7B5H0] % 国网-国网国际发展有限公司用户反馈电脑关机时出现蓝屏的问题 % 初次响应 CMIT: 0001575

王先生 您好:

查看您最新上传的 dump 文件，还是 0x9f 错误，只不过具体的报错参数有一点变化。

```
7: kd> !analyze -v
*******************************************************************************
*                                                                             *
*                        Bugcheck Analysis                                    *
*                                                                             *
*******************************************************************************

DRIVER_POWER_STATE_FAILURE (9f)
A driver has failed to complete a power IRP within a specific time.
Arguments:
Arg1: 0000000000000003, A device object has been blocking an Irp for too long a time
Arg2: ffffca0b09b4c360, Physical Device Object of the stack
Arg3: ffffca007548f790, nt!TRIAGE_9F_POWER on Win7 and higher, otherwise the Functional Device Object of the stack
Arg4: ffffcd0b11427010, The blocked IRP

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

Implicit thread is now ffffcd0b`05eba040
```

但最终还是出现 ndis!Ndis::BindEngine::ApplyBindChanges 递归调用造成线程死锁，确认是由 miniport binding 的 legacy WinPcap protocol **(npf)** driver 造成的。

```
0: kd> !mex.t ffffcd0b1bead080
Process                                 Thread                          CID       TEB              UserTime KernelTime ContextSwitch
eppcontainer.exe *32 (ffffcd0b1cef7080) ffffcd0b1bead080 (E|K|W|R|V) 271c.15cc 000000000024e000        0          0

WaitBlockList:
    Object           Type              Other Waiters
    ffffcd0b10bdb5b0 NotificationEvent             2

Irp List:
    IRP              File Driver
    ffffcd0b0e6f4c30      npf

 # Child-SP         Return           Call Site
 0 ffffca007c8366f0 fffff8045e256390 nt!KiSwapContext+0x76
 1 ffffca007c836830 fffff8045e2558bf nt!KiSwapThread+0x500
 2 ffffca007c8368e0 fffff8045e255163 nt!KiCommitThreadWait+0x14f
 3 ffffca007c836980 fffff804610d8670 nt!KeWaitForSingleObject+0x233
 4 ffffca007c836a70 fffff804610d1a49 ndis!KWaitEventBase<wistd::integral_constant<enum _EVENT_TYPE,0> >::Wait+0x28
 5 ffffca007c836ab0 fffff80461057f5c ndis!Ndis::BindEngine::ApplyBindChanges+0x12c69
 6 ffffca007c836b00 fffff804610e10b4 ndis!ndisOpenAdapterLegacyProtocol+0x270
 7 ffffca007c836cb0 fffff804610d2784 ndis!ndisBindLegacyProtocol+0x29c
 8 ffffca007c836e00 fffff804610c5c7b ndis!ndisRestartProtocol+0xda98
 9 ffffca007c836e70 fffff804610c5708 ndis!Ndis::BindEngine::Iterate+0x4c7
 a ffffca007c836ff0 fffff804610bedce ndis!Ndis::BindEngine::UpdateBindings+0x98
 b ffffca007c837040 fffff804610bee34 ndis!Ndis::BindEngine::DispatchPendingWork+0x76
 c ffffca007c837070 fffff80461057f5c ndis!Ndis::BindEngine::ApplyBindChanges+0x54
 d ffffca007c8370c0 fffff804610fbde3 ndis!ndisOpenAdapterLegacyProtocol+0x270
 e ffffca007c837270 fffff804757c2edd ndis!NdisOpenAdapter+0x63
 f ffffca007c8372e0 fffff8045e24ad55 npf+0x2edd
10 ffffca007c837390 fffff8045e261b24 nt!IofCallDriver+0x55
11 ffffca007c8373d0 fffff8045e63e3c1 nt!IoCallDriverWithTracing+0x34
12 ffffca007c837420 fffff8045e632517 nt!IopParseDevice+0x11c1
13 ffffca007c837580 fffff8045e63aaba nt!ObpLookupObjectName+0x1117
14 ffffca007c837750 fffff8045e629e7b nt!ObOpenObjectByNameEx+0x1fa
15 ffffca007c837880 fffff8045e627fa9 nt!IopCreateFile+0x132b
16 ffffca007c837940 fffff8045e412205 nt!NtCreateFile+0x79
17 ffffca007c8379d0 00007ffd1936e004 nt!KiSystemServiceCopyEnd+0x25
 0 00000000046cd978 00000000768b080b ntdll_77aa0000!NtCreateFile+0xc
 1 00000000046cd97c 00000000768b030e KERNELBASE!CreateFileInternal+0x4eb
 2 00000000046cda40 00000000768ad2e1 KERNELBASE!CreateFileW+0x5e
 3 00000000046cda70 00000000035637aa KERNELBASE!CreateFileA+0x31
 4 00000000046cdaa0 0000000770de41f Packet+0x37aa
 5 00000000046cdac0 0000000000000000 KERNEL32!GlobalUnlock+0xaf
```

这一次很详细的能看到 360safe 目录中的模块 Packet.dll 调用了 npf 驱动。

```
0: kd> lmvm Packet
Browse full module list
start             end                 module name
00000000`03560000 00000000`03578000   Packet     (export symbols)       Packet.dll
    Loaded symbol image file: Packet.dll
    Image path: C:\Program Files (x86)\360\360Safe\safemon\seccscan\Packet.dll
    Image name: Packet.dll
    Browse all global symbols  functions  data
    Timestamp:        Fri Mar  1 09:28:28 2013 (5130043C)
    CheckSum:         00019417
    ImageSize:        00018000
    File version:     4.1.0.2980
    Product version:  4.1.0.2980
    File flags:       0 (Mask 17)
    File OS:          4 Unknown Win32
    File type:        2.0 Dll
    File date:        00000000.00000000
    Translations:     0000.04b0
    Information from resource tables:
        CompanyName:      Riverbed Technology, Inc.
        ProductName:      WinPcap
        InternalName:     packet.dll
        OriginalFilename: packet.dll
        ProductVersion:   4.1.0.2980
        FileVersion:      4.1.0.2980
        FileDescription:  packet.dll (Vista) Dynamic Link Library
        LegalCopyright:   Copyright © 2010-2013 Riverbed Technology, Inc. Copyright © 2005-2010 CACE Technologies.
        LegalTrademarks:
```

后续建议：

1）与 360 方面确认有哪些功能或者策略修改需要使用 npf 驱动，是否可以对相关策略做调整。

2）尝试使用 npcap 替代 winpcap 功能，验证是否解决问题。

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: 2024 年 8 月 26 日 16:09
收件人: '王麦熟' <w13731242724@163.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: 回复: Re:回复: Re:回复: Re:回复: 回复: [案例号: CAS-11760-F7B5H0] % 国网-国网国际发展有限公司用户反馈电脑关机时出现蓝屏的问题 % 初次响应 CMIT: 0001575

王先生 您好:

查看您最新的 dump 文件，还是 0x9f 错误，电源状态转换因等待与 PnP 子系统同步**超时**导致了蓝屏。

出现 timeout 超时的原因是 ndis!Ndis::BindEngine::ApplyBindChanges 递归调用造成线程死锁，这个是由 miniport binding 的 legacy WinPcap protocol **(npf**) driver 造成的。

```
0: kd> !mex.t ffff8585f3dd9080
Process                                 Thread                          CID       TEB              UserTime KernelTime Co
eppcontainer.exe *32 (ffff8585f1e60080) ffff8585f3dd9080 (E|K|W|R|V) 1ab8.1e24 0000000000636000        0          0

WaitBlockList:
    Object           Type              Other Waiters
    ffff8585ebc395b0 NotificationEvent             1

Irp List:
    IRP              File Driver
    ffff8585f38f8380       npf

 # Child-SP         Return           Call Site
 0 ffff800c0cc6e530 fffff80722a1b840 nt!KiSwapContext+0x76
 1 ffff800c0cc6e670 fffff80722a1ad6f nt!KiSwapThread+0x500
 2 ffff800c0cc6e720 fffff80722a1a613 nt!KiCommitThreadWait+0x14f
 3 ffff800c0cc6e7c0 fffff80724fc7540 nt!KeWaitForSingleObject+0x233
 4 ffff800c0cc6e8b0 fffff80724fc0919 ndis!KWaitEventBase<wistd::integral_constant<enum _EVENT_TYPE,0> >::Wait+0x28
 5 ffff800c0cc6e8f0 fffff80724f4752c ndis!Ndis::BindEngine::ApplyBindChanges+0x12c69
 6 ffff800c0cc6e940 fffff80724fcff84 ndis!ndisOpenAdapterLegacyProtocol+0x270
 7 ffff800c0cc6eaf0 fffff80724fc1654 ndis!ndisBindLegacyProtocol+0x29c
 8 ffff800c0cc6ec40 fffff80724fb4b4b ndis!ndisRestartProtocol+0xda98
 9 ffff800c0cc6ecb0 fffff80724fb45d8 ndis!Ndis::BindEngine::Iterate+0x4c7
 a ffff800c0cc6ee30 fffff80724fadc9e ndis!Ndis::BindEngine::UpdateBindings+0x98
 b ffff800c0cc6ee80 fffff80724fadd04 ndis!Ndis::BindEngine::DispatchPendingWork+0x76
 c ffff800c0cc6eeb0 fffff80724f4752c ndis!Ndis::BindEngine::ApplyBindChanges+0x54
 d ffff800c0cc6ef00 fffff80724feade3 ndis!ndisOpenAdapterLegacyProtocol+0x270
 e ffff800c0cc6f0b0 fffff80739d02edd ndis!NdisOpenAdapter+0x63
 f ffff800c0cc6f120 fffff80722a329b5 npf+0x2edd
10 ffff800c0cc6f1d0 fffff80722a33fb4 nt!IofCallDriver+0x55
11 ffff800c0cc6f210 fffff80722e3b2ed nt!IoCallDriverWithTracing+0x34
```

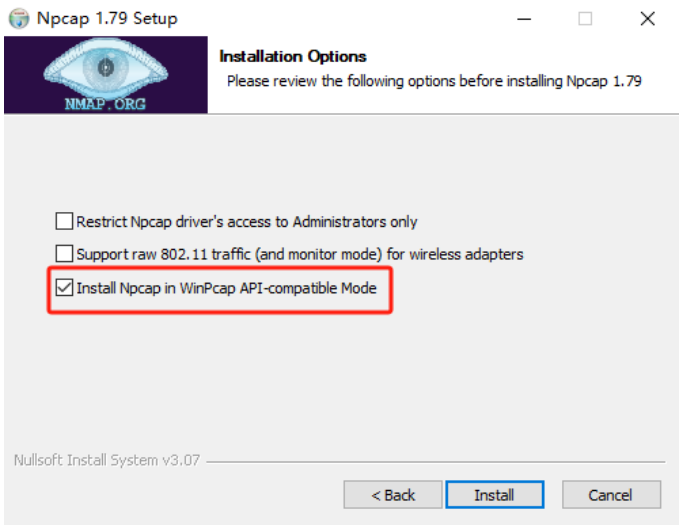
查看 npf.sys 驱动情况：

```
0: kd> lmvm npf
Browse full module list
start             end                 module name
fffff807`39d00000 fffff807`39d0c000   npf        (no symbols)
    Loaded symbol image file: npf.sys
    Image path: \??\C:\Windows\system32\drivers\npf.sys
    Image name: npf.sys
    Browse all global symbols  functions  data
    Timestamp:        Fri Mar  1 09:31:24 2013 (513004EC)
    CheckSum:         00017159
    ImageSize:        0000C000
    Translations:     0000.04b0 0000.04e4 0409.04b0 0409.04e4
    Information from resource tables:
```

查询了一些资料，可以**尝试使用 npcap 替代 winpcap 功能**：

https://npcap.com/#download

在安装 npcap 过程中，注意选择“WinPcap API-compatible Mode”，它会将自己的驱动替换 npf.sys 驱动。



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: 2024 年 8 月 22 日 16:55
收件人: '王麦熟' <w13731242724@163.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: 回复: Re:回复: Re:回复: Re:回复: 回复： [案例号: CAS-11760-F7B5H0] % 国网-国网国际发展有限公司用户反馈电脑关机时出现蓝屏的问题 % 初次响应 CMIT: 0001575

王先生 您好:

来信是想咨询当前案例进展情况。

如果有问题设备出现蓝屏问题，请您将问题设备的 **C:\Windows\memory.dmp** 文件压缩后，通过 CDUC 上传，提供给我们进一步排查，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: 2024 年 8 月 15 日 15:53
收件人: '王麦熟' <w13731242724@163.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: 回复: Re:回复: Re:回复: Re:回复: 回复： [案例号: CAS-11760-F7B5H0] % 国网-国网国际发展有限公司用户反馈电脑关机时出现蓝屏的问题 % 初次响应 CMIT: 0001575

王先生 您好:

来信是想咨询当前案例进展情况。

近期是否有已经删除了 npf.sys 驱动的设备再次出现蓝屏问题?

如果有问题设备出现蓝屏问题，请您将问题设备的 **C:\Windows\memory.dmp** 文件压缩后，通过 CDUC 上传，提供给我们进一步排查，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

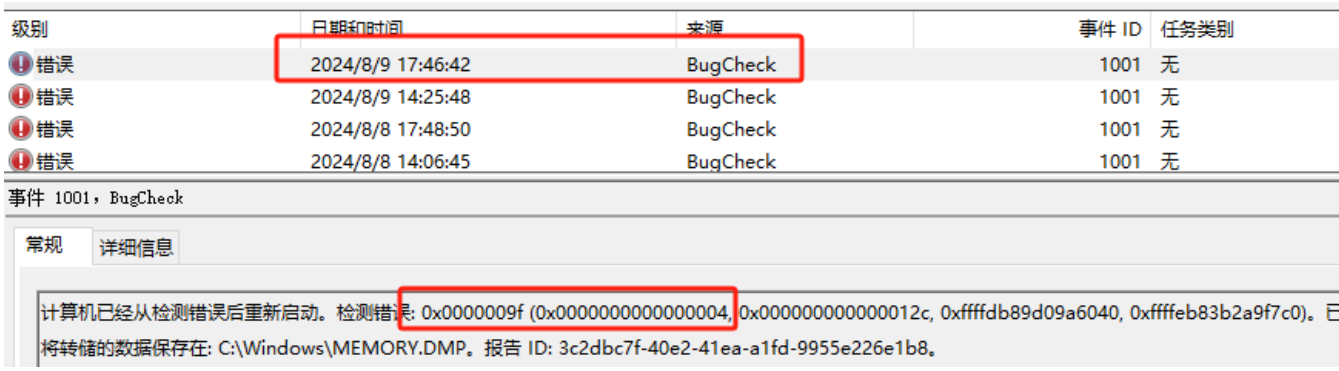
电子邮箱 Email: weiliang@cmgos.com

发件人: Wei Liang
发送时间: 2024 年 8 月 13 日 11:18
收件人: '王麦熟' <w13731242724@163.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: 回复: Re:回复: Re:回复: Re:回复: 回复： [案例号: CAS-11760-F7B5H0] % 国网-国网国际发展有限公司用户反馈电脑关机时出现蓝屏的问题 % 初次响应 CMIT: 0001575

王先生 您好:

感谢您的电话接听。

从您提供的系统日志可以看到最新的出现蓝屏的时间是 8 月 9 日 17 点 46 分多，更详细的问题排查还是需要拿到对应的 dump 文件分析。



您已经删除了此 dump 文件，需要**等待下一次再次出现蓝屏问题后，获取最新的 dump 文件**提供给我们进一步排查问题，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: 2024 年 8 月 8 日 17:05
收件人: '王麦熟' <w13731242724@163.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: 回复: Re:回复: Re:回复: Re:回复: 回复: [案例号: CAS-11760-F7B5H0] % 国网-国网国际发展有限公司用户反馈电脑关机时出现蓝屏的问题 % 初次响应 CMIT: 0001575

王先生 您好:

下载了您提供的最新的 memory.dump 文件，加载这个 **dump 显示数据损坏。**

```
Loading Dump File [\\10.0.18.49\log\CAS-11760-F7B5H0\MEMORY-3\MEMORY.DMP]
Kernel Bitmap Dump File: Kernel address space is available, User address space may not be available.


************* Path validation summary **************
Response                         Time (ms)     Location
Deferred                                       cache*\\10.0.37.113\共享文件\二线团队及流程资料\symbols
Deferred                                       srv*https://msdl.microsoft.com/download/symbols
Symbol search path is: cache*\\10.0.37.113\共享文件\二线团队及流程资料\symbols;srv*https://msdl.microsoft.com/download/symbols
Executable search path is:
Missing image name, possible paged-out or corrupt data.
Unable to load image Unknown_Module_00000000`00000000, Win32 error 0n2
*** WARNING: Unable to verify timestamp for Unknown_Module_00000000`00000000
*** ERROR: Module load completed but symbols could not be loaded for Unknown_Module_00000000`00000000
Unable to add module at 00000000`00000000
WARNING: .reload failed, module list may be incomplete
```

无法基于此 dump 进一步排查，而且此 dump 文件压缩后只有 26MB 左右，与上两个 dump 文件压缩后的大小有较大的差异。

请您在问题设备上**删除这个有问题的 dump 文件，再次复现蓝屏问题后提供新的 dump 日志**给 CMIT 进一步分析。

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: 2024 年 8 月 7 日 15:03
收件人: '王麦熟' <w13731242724@163.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: 回复: Re:回复: Re:回复: Re:回复: 回复： [案例号: CAS-11760-F7B5H0] % 国网-国网国际发展有限公司用户反馈电脑关机时出现蓝屏的问题 % 初次响应 CMIT: 0001575

王先生 您好:

感谢您的电话接听。

如电话中所说，请您测试在问题设备上移除了 npf.sys 驱动后，确认是否能解决蓝屏问题，从 dump 分析和实际测试两方面明确是 npf.sys 驱动导致的关机蓝屏问题。

如果问题设备删除 npf.sys 驱动后还是出现蓝屏问题，您可以再次将蓝屏 dump 压缩后发送给 CMIT 进一步排查。

如测试明确确认了是 npf 驱动导致的蓝屏问题，再与三方应用厂商沟通是否可以升级此驱动，或者使用其他的抓包工具驱动替代 npf.sys 驱动功能

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: 2024 年 8 月 5 日 17:50
收件人: '王麦熟' <w13731242724@163.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: 回复: Re:回复: Re:回复: Re:回复: 回复： [案例号: CAS-11760-F7B5H0] % 国网-国网国际发展有限公司用户反馈电脑关机时出现蓝屏的问题 % 初次响应 CMIT: 0001575

王先生 您好:

感谢您的电话接听。

经过您的测试排查，确认 npf.sys 驱动是北信源管控软件引入的。请您与北信源沟通是否可以升级此驱动，或者使用其他的抓包工具替代 npf.sys 驱动功能。

如果无法确认是否一定需要 npf 驱动，您可以尝试删除 npf.sys 驱动，确认是否能解决关机蓝屏问题，且管控软件能正常工作，不影响用户正常使用设备。

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: 2024 年 8 月 2 日 16:48
收件人: '王麦熟' <w13731242724@163.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: 回复: Re:回复: Re:回复: Re:回复: 回复：[案例号: CAS-11760-F7B5H0] % 国网-国网国际发展有限公司用户反馈电脑关机时出现蓝屏的问题 % 初次响应 CMIT: 0001575

王先生 您好:

刚刚给您的电话没有接通。

测试重命名 npf.sys 驱动后，是否可以解决关机蓝屏问题。

是否已经排查到是哪一个三方应用引入的 npf.sys 驱动，与三方应用厂商沟通是否能升级驱动或者有其他的驱动替代 npf.sys 驱动。

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: 2024 年 7 月 31 日 17:37
收件人: '王麦熟' <w13731242724@163.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: 回复: Re:回复: Re:回复: Re:回复: 回复：[案例号: CAS-11760-F7B5H0] % 国网-国网国际发展有限公司用户反馈电脑关机时出现蓝屏的问题 % 初次响应 CMIT: 0001575

王先生 您好:

感谢您的电话接听。

如电话中所说，现在判断是 npf.sys 驱动导致的关机蓝屏问题，您可以在问题设备上测试将 npf.sys 驱动重命名后，再测试是否会出现关机蓝屏问题。

如果无法重命名 npf.sys，可以在 PE 环境下重命名此文件。npf.sys 文件路径为:

C:\Windows\System32\drivers\npf.sys

也可以观察、跟踪其他问题设备在**更新了网卡驱动后，再次出现蓝屏问题的概率。**

为了测试是哪个应用引入的 npf.sys 驱动，您可以安装纯净的操作系统后，再逐一安装所需的应用，确认是哪一个应用需要 npf.sys 驱动。

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: 2024 年 7 月 25 日 11:53
收件人: 王麦熟 <w13731242724@163.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: 回复: Re:回复: Re:回复: Re:回复: 回复： [案例号: CAS-11760-F7B5H0] % 国网-国网国际发展有限公司用户反馈电脑关机时出现蓝屏的问题 % 初次响应 CMIT: 0001575

王先生 您好:

排查您新上传的 dump 文件，与上一次的问题设备一样，报错 9f，也是由于 NDIS 的相关问题导致的蓝屏问题。

在**排查三方驱动 npf.sys 后，也可以尝试更新网卡驱动**，验证是否可以解决蓝屏问题。

从 dump 信息看，npf.sys 驱动有可能是 360 安全软件引入的，也可以和应用厂商沟通这个问题，是否有解决方法。

```
# Child-SP         Return           Call Site
0 ffffa6841a1de460 fffff80317f5a137 nt!KiSwapContext+0x76
1 ffffa6841a1de5a0 fffff80317f59ca9 nt!KiSwapThread+0x297
2 ffffa6841a1de660 fffff80317f58a30 nt!KiCommitThreadWait+0x549
3 ffffa6841a1de700 fffff8032e3f4320 nt!KeWaitForSingleObject+0x520
4 ffffa6841a1de7d0 fffff8032e3d3d63 ndis!KWaitEventBase<wistd::integral_constant<enum _EVENT_TYPE,0> >::Wait+0x28
5 ffffa6841a1de810 fffff8032e35e614 ndis!Ndis::BindEngine::ApplyBindChanges+0x14a03
6 ffffa6841a1de860 fffff8032e3fcc7f ndis!ndisOpenAdapterLegacyProtocol+0x20c
7 ffffa6841a1dea20 fffff8032e3d5558 ndis!ndisBindLegacyProtocol+0x297
8 ffffa6841a1deb70 fffff8032e3bfed6 ndis!ndisRestartProtocol+0x132e8
9 ffffa6841a1dec90 fffff8032e3bf657 ndis!Ndis::BindEngine::Iterate+0x60a
a ffffa6841a1dedf0 fffff8032e3c2091 ndis!Ndis::BindEngine::UpdateBindings+0x7b
b ffffa6841a1dee20 fffff8032e3bf3b4 ndis!Ndis::BindEngine::DispatchPendingWork+0x75
c ffffa6841a1dee50 fffff8032e35e614 ndis!Ndis::BindEngine::ApplyBindChanges+0x54
d ffffa6841a1deea0 fffff8032e4168dc ndis!ndisOpenAdapterLegacyProtocol+0x20c
e ffffa6841a1df060 fffff8032ff62edd ndis!NdisOpenAdapter+0x4c
f ffffa6841a1df0d0 fffff80317f9fc25 npf+0x2edd
10 ffffa6841a1df180 fffff80317fa1014 nt!IofCallDriver+0x59
11 ffffa6841a1df1c0 fffff8031852d102 nt!IoCallDriverWithTracing+0x34
12 ffffa6841a1df210 fffff803185014d9 nt!IopParseDevice+0x632
13 ffffa6841a1df380 fffff803184ffadf nt!ObpLookupObjectName+0x719
14 ffffa6841a1df550 fffff80318453a52 nt!ObOpenObjectByNameEx+0x1df
15 ffffa6841a1df690 fffff80318453219 nt!IopCreateFile+0x822
16 ffffa6841a1df730 fffff8032fd43ba9 nt!NtCreateFile+0x79
17 ffffa6841a1df7c0 fffff80318077105 360Hvm64+0x13ba9
18 ffffa6841a1df990 00007ffa10670204 nt!KiSystemServiceCopyEnd+0x25
19 0000000004b5e3e8 0000000000000000 0x7ffa10670204
```

dump 具体分析：

显示的蓝屏代码为 9f，这表明表明驱动程序处于不一致或无效的电源状态。

```
0: kd> !analyze -v
*******************************************************************************
*                                                                             *
*                        Bugcheck Analysis                                    *
*                                                                             *
*******************************************************************************

DRIVER_POWER_STATE_FAILURE (9f)
A driver has failed to complete a power IRP within a specific time.
Arguments:
Arg1: 0000000000000004, The power transition timed out waiting to synchronize with the Pnp
    subsystem.
Arg2: 000000000000012c, Timeout in seconds.
Arg3: ffffd90923d94600, The thread currently holding on to the Pnp lock.
Arg4: fffff8031b45c800, nt!TRIAGE_9F_PNP on Win7 and higher

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

查看详细的 dump 分析信息，arg1 等于 4，出现这个蓝屏问题的原因是电源状态转换超时，等待与 PnP 子系统同步。

查看资源锁的情况，也显示了与 thread ffffd90923d94600 有关。

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

Resource @ nt!IopDeviceTreeLock (0xfffff803182e0da0)    Shared 1 owning threads
    Contention Count = 1
     Threads: ffffd90923d94600-01<*>
KD: Scanning for held locks.

Resource @ nt!PiEngineLock (0xfffff803182e0ea0)    Exclusively owned
    Contention Count = 50
    NumberOfExclusiveWaiters = 3
     Threads: ffffd90923d94600-01<*>

     Threads Waiting On Exclusive Access:
              ffffd9091c1e8080       ffffd90923e8a080       ffffd90923dad040
KD: Scanning for held locks.....................................................

Resource @ 0xffffd9091bd1db10    Exclusively owned
    Contention Count = 31
     Threads: ffffd909187ba040-01<*>
KD: Scanning for held locks.....................................................

Resource @ 0xffffd9091b0aeb90    Exclusively owned
     Threads: ffffd909187ba040-01<*>
KD: Scanning for held locks.....................................................
35221 total locks, 4 locks currently held
```

排查 dump 中的具体信息，查看 thread ffffd90923d94600 的情况。

```
0: kd> !mex.t ffffd90923d94600
Process                 Thread                  CID      UserTime KernelTime ContextSwitches Wait Reason      Time State
System (ffffd9090d6b7080) ffffd90923d94600 (E|K|W|R|V) 4.37b8          0       47ms            4908 Executive   5m:00.015 Waiting

WaitBlockList:
   Object           Type             Other Waiters
   ffffd909188e85d8 NotificationEvent            1

Priority:
    Current Base Decrement ForegroundBoost IO Page
    15      12   0         0               0  5

 # Child-SP         Return           Call Site
 0 ffffa68418d86ec0 fffff80317f5a137 nt!KiSwapContext+0x76
 1 ffffa68418d87000 fffff80317f59ca9 nt!KiSwapThread+0x297
 2 ffffa68418d870c0 fffff80317f58a30 nt!KiCommitThreadWait+0x549
 3 ffffa68418d87160 fffff8032e3f4320 nt!KeWaitForSingleObject+0x520
 4 ffffa68418d87230 fffff8032e3d3d63 ndis!KWaitEventBase<wistd::integral_constant<enum _EVENT_TYPE,0> >::Wait+0x28
 5 ffffa68418d87270 fffff8032e3b278d ndis!Ndis::BindEngine::AddIVBindChanges+0x14803
```

查询其 WaitBlockList 情况，显示 Waiters 情况，都是在等待

ndis!KWaitEventBase<wistd::integral_constant<enum _EVENT_TYPE,0> >::Wait+0x28

```
0: kd> !mex.obj -waiters ffffd909188e85d8
Process              Thread             Id CSwitches User Kernel State           Time Reason    Wait Function
==================== ================== ==== ======== ==== ====== ======= ============ ======== ==============
eppcontainer.exe *32 ffffd9091ec2a080 c34         9    0      0 Waiting 9h:55:46.359 Executive ndis!KWaitEvent
System               ffffd90923d94600 37b8      4908    0   47ms Waiting    5m:00.015 Executive ndis!KWaitEvent
```

这显示与 NDIS 有关，NDIS 的全称是 "Network Driver Interface Specification"，即“网络驱动程序接口规范"，用于在操作系统上实现网络设备驱动程序。

查看 NDIS 中加载的相关协议驱动情况，查看是否有三方的驱动信息。

```
ffffd9091ab47a30 - WANARP

ffffd9091ab41a30 - RSPNDR
  ffffd9091aa849a0 - Intel(R) Ethernet Connection (11) I219-LM

ffffd9091ab349e0 - LLTDIO
  ffffd9091aa839a0 - Intel(R) Ethernet Connection (11) I219-LM

ffffd9091d88e010 - MSLLDP
  ffffd9091d93e9a0 - Intel(R) Ethernet Connection (11) I219-LM

ffffd90918359010 - 360ANTIARPPROT
  ffffd9091fa2b9a0 - Intel(R) Ethernet Connection (11) I219-LM

ffffd90918610010 - PACKETDRIVER

ffffd9090e8253a0 - PACKETDRIVER

ffffd9091805b8a0 - RDMANDK

ffffd9091813fbf0 - TCPIP6TUNNEL

ffffd9090e926010 - TCPIPTUNNEL

ffffd90916ec2bb0 - TCPIP6
  ffffd9091861b820 - Intel(R) Ethernet Connection (11) I219-LM

ffffd90918137bf0 - TCPIP
  ffffd9091861b440 - Intel(R) Ethernet Connection (11) I219-LM
```

这三个对应的驱动是 360LanProtect.sys、EdpPcap.sys 和 npf.sys。查看驱动详细信息如下。

```
0: kd> lmvm 360LanProtect
Browse full module list
start             end                 module name
fffff803`30ea0000 fffff803`30ee6000   360LanProtect   (no symbols)
    Loaded symbol image file: 360LanProtect.sys
    Image path: \SystemRoot\System32\drivers\360LanProtect.sys
    Image name: 360LanProtect.sys
    Browse all global symbols  functions  data
    Timestamp:        Mon Feb  1 15:41:25 2021 (6017B0A5)
    CheckSum:         0001B8FC
    ImageSize:        00046000
    Translations:     0000.04b0 0000.04e4 0409.04b0 0409.04e4
    Information from resource tables:
0: kd> lmvm edppcap
Browse full module list
start             end                 module name
fffff803`2ffa0000 fffff803`2ffac000   EdpPcap    (deferred)
    Image path: \SystemRoot\System32\Drivers\EdpPcap.sys
    Image name: EdpPcap.sys
    Browse all global symbols  functions  data
    Timestamp:        Tue Apr 26 12:59:06 2016 (571EF59A)
    CheckSum:         000125EC
    ImageSize:        0000C000
    Translations:     0000.04b0 0000.04e4 0409.04b0 0409.04e4
    Information from resource tables:
0: kd> lmvm npf
Browse full module list
start             end                 module name
fffff803`2ff60000 fffff803`2ff6c000   npf        (no symbols)
    Loaded symbol image file: npf.sys
    Image path: \??\C:\Windows\system32\drivers\npf.sys
    Image name: npf.sys
    Browse all global symbols  functions  data
    Timestamp:        Fri Mar  1 09:31:24 2013 (513004EC)
    CheckSum:         00017139
    ImageSize:        0000C000
    Translations:     0000.04b0 0000.04e4 0409.04b0 0409.04e4
```

EdpPcap.sys 和 npf.sys 驱动的时间较老，**建议询问三方厂商是否可以升级这两个驱动版本。**

查看网卡驱动版本，也建议升级网卡驱动后观察是否解决问题。

```
0: kd> lmvm  e1d68x64
Browse full module list
start             end                 module name
fffff803`39400000 fffff803`39496000   e1d68x64   (deferred)
    Image path: \SystemRoot\System32\DriverStore\FileRepository\e1d68x64.inf_amd64_f0a10bbc2f94fc6b\e1d68x64.sys
    Image name: e1d68x64.sys
    Browse all global symbols  functions  data
    Timestamp:        Tue Feb  4 01:25:31 2020 (5E38578B)
    CheckSum:         000953F7
    ImageSize:        00096000
    Translations:     0000.04b0 0000.04e4 0409.04b0 0409.04e4
    Information from resource tables:
```

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: 2024 年 7 月 24 日 17:24
收件人: 王麦熟 <w13731242724@163.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: 回复: Re:回复: Re:回复: Re:回复: 回复： [案例号: CAS-11760-F7B5H0] % 国网-国网国际发展有限公司用户反馈电脑关机时出现蓝屏的问题 % 初次响应 CMIT: 0001575

王先生 您好:

您上传的日志已经收到，我们正在分析排查，有任何进展会及时与您沟通，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: 王麦熟 <w13731242724@163.com>
发送时间: 2024 年 7 月 24 日 17:20
收件人: Wei Liang <weiliang@cmgos.com>
主题: Re:回复: Re:回复: Re:回复: 回复： [案例号: CAS-11760-F7B5H0] % 国网-国网国际发展有限公司用户反馈电脑关机时出现蓝屏的问题 % 初次响应 CMIT: 0001575

压缩上传完成

在 2024-07-24 17:17:12，"Wei Liang" <weiliang@cmgos.com> 写道：

> 王先生 您好:
>
> 如果上传数据确实太慢，您可以先尝试在本地压缩后再上传，先测试 dump 文件压缩后可以节省很多空间。
>
> 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: 王麦熟 <w13731242724@163.com>
发送时间: 2024 年 7 月 24 日 17:13
收件人: Wei Liang <weiliang@cmgos.com>
主题: Re:回复: Re:回复: 回复： [案例号: CAS-11760-F7B5H0] % 国网-国网国际发展有限公司用户反馈电脑关机时出现蓝屏的问题 % 初次响应 CMIT: 0001575

上传数据特别慢

在 2024-07-24 16:46:55，"Wei Liang" <weiliang@cmgos.com> 写道：

> 王先生 您好:
>
> 我现在还没有看到您上传的日志，等您上传完毕后我再下载排查。您现在提供的 dump 日志是不是新的问题设备吗？还是就是原先的那一台设备？
>
> 原先的那台设备的测试结果怎样，有什么进展？

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: 王麦熟 <w13731242724@163.com>
发送时间: 2024 年 7 月 24 日 16:32
收件人: Wei Liang <weiliang@cmgos.com>
主题: Re:回复: 回复： [案例号: CAS-11760-F7B5H0] % 国网-国网国际发展有限公司用户反馈电脑关机时出现蓝屏的问题 % 初次响应 CMIT: 0001575

你好 危亮工程师
我又抓了一个日志上传了你在给分析一下

在 2024-07-23 10:38:13，"Wei Liang" <weiliang@cmgos.com> 写道：

> 王先生 您好:
>
> 感谢您的电话接听。
>
> 如电话中所说，您可以先**更新网卡驱动，再测试验证**是否能解决关机时蓝屏的问题。

从 dump 信息看，npf.sys 驱动有可能是 360 安全软件引入的，也可以和应用厂商沟通这个问题，是否有解决方法。

```
# Child-SP          Return           Call Site
0 ffff9809697ae530 fffff8057bc0c800 nt!KiSwapContext+0x76
1 ffff9809697ae670 fffff8057bc0bd2f nt!KiSwapThread+0x500
2 ffff9809697ae720 fffff8057bc0b5d3 nt!KiCommitThreadWait+0x14f
3 ffff9809697ae7c0 fffff805805b7540 nt!KeWaitForSingleObject+0x233
4 ffff9809697ae8b0 fffff805805b0919 ndis!KWaitEventBase<wistd::integral_constant<enum _EVENT_TYPE,0> >::Wait+0x28
5 ffff9809697ae8f0 fffff8058053752c ndis!Ndis::BindEngine::ApplyBindChanges+0x12c69
6 ffff9809697ae940 fffff805805bff84 ndis!ndisOpenAdapterLegacyProtocol+0x270
7 ffff9809697aeaf0 fffff805805b1654 ndis!ndisBindLegacyProtocol+0x29c
8 ffff9809697aec40 fffff805805a4b4b ndis!ndisRestartProtocol+0xda98
9 ffff9809697aecb0 fffff805805a45d8 ndis!Ndis::BindEngine::Iterate+0x4c7
a ffff9809697aee30 fffff8058059dc9e ndis!Ndis::BindEngine::UpdateBindings+0x98
b ffff9809697aee80 fffff8058059dd04 ndis!Ndis::BindEngine::DispatchPendingWork+0x76
c ffff9809697aeeb0 fffff8058053752c ndis!Ndis::BindEngine::ApplyBindChanges+0x54
d ffff9809697aef00 fffff805805dade3 ndis!ndisOpenAdapterLegacyProtocol+0x270
e ffff9809697af0b0 fffff805947c2edd ndis!NdisOpenAdapter+0x63
f ffff9809697af120 fffff8057bc8f835 npf+0x2edd
10 ffff9809697af1d0 fffff8057bc90e34 nt!IofCallDriver+0x55
11 ffff9809697af210 fffff8057c07891d nt!IoCallDriverWithTracing+0x34
12 ffff9809697af260 fffff8057bff307e nt!IopParseDevice+0x117d
13 ffff9809697af3d0 fffff8057c095fda nt!ObpLookupObjectName+0x3fe
14 ffff9809697af5a0 fffff8057c016e2f nt!ObOpenObjectByNameEx+0x1fa
15 ffff9809697af6d0 fffff8057c016a09 nt!IopCreateFile+0x40f
16 ffff9809697af770 fffff805945a3ba9 nt!NtCreateFile+0x79
17 ffff9809697af800 fffff8057be08fb5 360Hvm64+0x13ba9
18 ffff9809697af9d0 00007ffdb67ed814 nt!KiSystemServiceCopyEnd+0x25
19 0000000007d1e568 0000000000000000 0x7ffdb67ed814
```

至于其他的设备出现的蓝屏问题，请您按照最开始的邮件说明，将蓝屏 dump 文件提供给我们进一步排查，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: 2024 年 7 月 22 日 16:06
收件人: '王麦熟' <w13731242724@163.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: 回复: 回复： [案例号: CAS-11760-F7B5H0] % 国网-国网国际发展有限公司用户反馈电脑关机时出现蓝屏的问题 % 初次响应 CMIT: 0001575

王先生 您好:

刚刚给您的电话没有接通。

来信是想询问当前案例进展。如上次的邮件所说，dump 日志显示蓝屏与 NDIS 有关，这是网络相关的问题。

在排查三方驱动 EdpPcap.sys 和 npf.sys 后，也可以尝试更新网卡驱动，请问这些验证测试是否可以解决蓝屏问题。

如果有任何进展或疑问可以回复此邮件，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: 2024 年 7 月 18 日 14:34
收件人: '王麦熟' <w13731242724@163.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: 回复: 回复： [案例号: CAS-11760-F7B5H0] % 国网-国网国际发展有限公司用户反馈电脑关机时出现蓝屏的问题 % 初次响应 CMIT: 0001575

王先生 您好:

感谢您的电话接听。

如上一封邮件所说，dump 日志显示蓝屏与 NDIS 有关，这是网络相关的问题。

除了**排查三方驱动 EdpPcap.sys 和 npf.sys，**也可以尝试更新**网卡驱动**，验证是否可以解决问题。

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: 2024 年 7 月 18 日 11:33
收件人: '王麦熟' <w13731242724@163.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: 回复: 回复： [案例号: CAS-11760-F7B5H0] % 国网-国网国际发展有限公司用户反馈电脑关机时出现蓝屏的问题 % 初次响应 CMIT: 0001575

王先生 您好:

查看您提供的 dump 文件，显示的蓝屏代码为 9f，这表明表明驱动程序处于不一致或无效的电源状态。

```
12: kd> !analyze -v
*******************************************************************************
*                                                                             *
*                        Bugcheck Analysis                                    *
*                                                                             *
*******************************************************************************

DRIVER_POWER_STATE_FAILURE (9f)
A driver has failed to complete a power IRP within a specific time.
Arguments:
Arg1: 0000000000000004, The power transition timed out waiting to synchronize with the Pnp
    subsystem.
Arg2: 000000000000012c, Timeout in seconds.
Arg3: ffffbc8fcab5a580, The thread currently holding on to the Pnp lock.
Arg4: ffff9809676df7c0, nt!TRIAGE_9F_PNP on Win7 and higher

Debugging Details:
```

查看详细的 dump 分析信息，arg1 等于 4，出现这个蓝屏问题的原因是电源状态转换超时，等待与 PnP 子系统同步。

查看资源锁的情况，也显示了与 thread ffffbc8fcab5a580 有关。

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

Resource @ nt!IopDeviceTreeLock (0xfffff8057c644a60)    Shared 1 owning threads
     Threads: ffffbc8fcab5a580-01<*>
KD: Scanning for held locks.

Resource @ nt!PiEngineLock (0xfffff8057c644b60)    Exclusively owned
    Contention Count = 47
    NumberOfExclusiveWaiters = 2
     Threads: ffffbc8fcab5a580-01<*>

     Threads Waiting On Exclusive Access:
              ffffbc8fc0bdf080       ffffbc8fc6637040
KD: Scanning for held locks.....................................................

Resource @ 0xffffbc8fc0a09590    Exclusively owned
    Contention Count = 62
     Threads: ffffbc8fbd3e7280-01<*>
KD: Scanning for held locks.....................................

Resource @ 0xffffbc8fc34cb710    Exclusively owned
    Contention Count = 4
     Threads: ffffbc8fbd3e7280-01<*>
KD: Scanning for held locks.....................................................
52270 total locks, 4 locks currently held
```

排查 dump 中的具体信息，查看 thread ffffbc8fcab5a580 的情况。

```
0: kd> !mex.t ffffbc8fcab5a580
Process                 Thread                  CID      UserTime KernelTime ContextSwitches Wait Reason      Tim
System (ffffbc8fb62b10c0) ffffbc8fcab5a580 (E|K|W|R|V) 4.1518          0       63ms            6758 Executive   5m:00.01

WaitBlockList:
    Object           Type              Other Waiters
    ffffbc8fbd8765b0 NotificationEvent             1

Priority:
    Current Base Decrement ForegroundBoost IO Page
    15      12   0         0               0  5
```

查询其 WaitBlockList 情况，显示 Waiters 情况，都是在等待

ndis!KWaitEventBase<wistd::integral_constant<enum _EVENT_TYPE,0> >::Wait+0x28

```
0: kd> !mex.obj -waiters ffffbc8fbd8765b0
Process              Thread             Id CSwitches User Kernel State         Time Reason
==================== ================== ==== ========= ==== ====== ======= ========== =========
eppcontainer.exe *32 ffffbc8fc9b3a080 362c         6    0      0 Waiting 28m:42.703 Executive
System               ffffbc8fcab5a580 1518      6758    0   63ms Waiting  5m:00.015 Executive
```

这显示与 NDIS 有关。NDIS 的全称是 "Network Driver Interface Specification"，即“网络驱动程序接口规范”，是一种标准化接口规范，用于在操作系统上实现网络设备驱动程序。

查看 NDIS 中加载的相关协议驱动情况，查看是否有三方的驱动信息。

```
ffffbc8fc3b88b60 - WANARP

ffffbc8fc3b79920 - RSPNDR
  ffffbc8fbdbe13a0 - Intel(R) Ethernet Connection (17) I219-LM

ffffbc8fc3b72a20 - LLTDIO
  ffffbc8fbdccba70 - Intel(R) Ethernet Connection (17) I219-LM

ffffbc8fc37f4a20 - MSLLDP
  ffffbc8fb637fa60 - Intel(R) Ethernet Connection (17) I219-LM

ffffbc8fb9f24bf0 - 360ANTIARPPROT
  ffffbc8fc96e4a20 - Intel(R) Ethernet Connection (17) I219-LM

ffffbc8fb9f88a30 - PACKETDRIVER

ffffbc8fb9f448a0 - PACKETDRIVER

ffffbc8fbd1b8010 - RDMANDK

ffffbc8fb9b76bf0 - TCPIP6TUNNEL

ffffbc8fb99de8e0 - TCPIPTUNNEL

ffffbc8fb99778a0 - TCPIP6
  ffffbc8fbda93b30 - Intel(R) Ethernet Connection (17) I219-LM
```

这三个对应的驱动是 360LanProtect.sys、EdpPcap.sys 和 npf.sys。查看驱动详细信息如下。

```
0: kd> lmvm 360LanProtect
Browse full module list
start             end                 module name
fffff805`93ff0000 fffff805`94036000   360LanProtect   (no symbols)
    Loaded symbol image file: 360LanProtect.sys
    Image path: \SystemRoot\System32\drivers\360LanProtect.sys
    Image name: 360LanProtect.sys
    Browse all global symbols  functions  data
    Timestamp:        Mon Feb  1 15:41:25 2021 (6017B0A5)
    CheckSum:         0001B8FC
    ImageSize:        00046000
    Translations:     0000.04b0 0000.04e4 0409.04b0 0409.04e4
    Information from resource tables:
```

```
0: kd> lmvm edppcap
Browse full module list
start             end                 module name
fffff805`93e00000 fffff805`93e0c000   EdpPcap    (no symbols)
    Loaded symbol image file: EdpPcap.sys
    Image path: \SystemRoot\System32\Drivers\EdpPcap.sys
    Image name: EdpPcap.sys
    Browse all global symbols  functions  data
    Timestamp:        Tue Apr 26 12:59:06 2016 (571EF59A)
    CheckSum:         000125EC
    ImageSize:        0000C000
    Translations:     0000.04b0 0000.04e4 0409.04b0 0409.04e4
    Information from resource tables:
```

```
0: kd> lmvm npf
Browse full module list
start             end                 module name
fffff805`947c0000 fffff805`947cc000   npf        (no symbols)
    Loaded symbol image file: npf.sys
    Image path: \??\C:\Windows\system32\drivers\npf.sys
    Image name: npf.sys
    Browse all global symbols  functions  data
    Timestamp:        Fri Mar 1 09:31:24 2013 (513004EC)
    CheckSum:         00017139
    ImageSize:        0000C000
    Translations:     0000.04b0 0000.04e4 0409.04b0 0409.04e4
    Information from resource tables:
```

EdpPcap.sys 和 npf.sys 驱动的时间较老，**建议询问三方厂商是否可以升级这两个驱动版本。也可以测试不安装这两个驱动是否能正常关机。**

查询到 EdpPcap.sys 是北信源的驱动，而 npf.sys 应该是三方的一个抓包工具的驱动。

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: 王麦熟 <w13731242724@163.com>
发送时间: 2024 年 7 月 18 日 10:38
收件人: Wei Liang <weiliang@cmgos.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: 回复：[案例号: CAS-11760-F7B5H0]% 国网-国网国际发展有限公司用户反馈电脑关机时出现蓝屏的问题 % 初次响应 CMIT: 0001575

你好，我想咨询一下，什么时候能出结果和方案，有一台电脑回复出厂设置，过几天又重新复现管理关不上的问题

---- 回复的原邮件 ----

发件人	Wei Liang<weiliang@cmgos.com>
发送日期	2024 年 07 月 17 日 15:54
收件人	王麦熟 <w13731242724@163.com>
抄送人	PR_Case_Notification <pr_case_notification@cmgos.com>
主题	回复: Re:回复: [案例号: CAS-11760-F7B5H0] % 国网-国网国际发展有限公司用户反馈电脑关机时出现蓝屏的问题 % 初次响应 CMIT:0001575

王先生 您好:

你提供的日志已经收到，我们正在分析排查，有任何进展会及时与您沟通，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: 王麦熟 <w13731242724@163.com>
发送时间: 2024 年 7 月 17 日 15:05
收件人: Wei Liang <weiliang@cmgos.com>
主题: Re:回复: [案例号: CAS-11760-F7B5H0] % 国网-国网国际发展有限公司用户反馈电脑关机时出现蓝屏的问题 % 初次响应 CMIT:0001575

蓝屏日志上传完成

在 2024-07-16 15:15:00，"Wei Liang" <weiliang@cmgos.com> 写道：

> 王先生 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:

国网国际用户反馈有多台设备关机时出现蓝屏问题，核实蓝屏代码为DRIVER_POWER_STATE_FAILURE，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。

请您从以下链接下载相关的工具，在问题设备上按照相关操作收集日志，并通过 CDUC 上传。

CMGElogCollectorV2 工具：
https://cduc.cmgos.com/download.php?id=1458&token=PcEQH06HPAu7P3p5paWBqHjWbwlqLJdc

1）找一台问题设备，解压 CMGETool 后双击运行 **CMGELogCollectorV2.exe，**选择**内存转储配置**，按照以下设置配置完全内存转储。

2）点击设置完成后，需要**重启设备使设置生效。**

3）先关机复现蓝屏问题，待设备保存 dump 后，是否能自动重启进入系统，如果无法自动重启，等待一段时间后强制重启。

4）在问题设备上，解压 CMGETool 后双击运行 **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。

5）查看 C:\Windows\memory.dmp 文件，确认此文件是最新生成的，将 **memory.dmp 文件压缩**后通过 CDUC 上传。

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。

（用户名密码区分大小写）

用户名：gwguoji

密码：gwguoji

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

神州网信
CMIT

发件人: Wei Liang <weiliang@cmgos.com>
发送时间: 2024 年 7 月 16 日 14:59
收件人: 王先生 <w13731242724@163.com>
抄送: Wei Liang <weiliang@cmgos.com>
主题: [案例号：CAS-11760-F7B5H0] % 国网-国网国际发展有限公司用户反馈电脑关机时出现蓝屏的问题 % 初次响应 CMIT:0001575

王先生 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-11760-F7B5H0 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

以上内容是一封有关向神州网信技术有限公司提交技术支持事件的邮件。

如果您希望本次回复能够被自动加入技术支持事件中,您可以选择“全部回复”。