

覃先生, 张先生 您好!

很高兴收到您的邮件, 根据反馈的结果, 我将暂时归档此问题。**案例归档后您会收到调查问卷的邮件, 希望可以对我们的服务进行评价。**

工单的归档并不会影响我们为您提供技术支持服务, 如果您的问题复现, 或有新的问题出现, 您也可以致电我们的技术支持热线 4008180055。

案例总结:

案例描述:

经销商为用户重装系统, 使用一段时间后电脑发生蓝屏问题,

联想客服检查排除硬件问题, 经销商反馈, 用户只安装日常办公软件, 无安装特殊软件和驱动程序

解决方案:

卸载现有显卡驱动, 安装其他无蓝屏问题稳定版本的显卡驱动, 问题不再复现。

案例分析:

- 目前看到系统事件日志有大量蓝屏 Bugcheck 报错, 本次的报错为 0x0000004a。其余多次各不相同, 例如: 0x0000007e、0x00000051、0x000000ef 等。
- 蓝屏问题触发时, 每次会生成一个 MEMORY.DMP 文件。当前只针对本次生成的 Bugcheck 为 0x0000004a 的问题进行分析, 分析结果不代表其他蓝屏问题的原因。

System 20 事件数: 15,293				
已筛选: 日志: file://D:\Logs\CAS-04004-H2H1M1\20210422_082451\EventLog\System.evtx; 级别: 关键, 错误, 警告; 来源: Microsoft-Windows-WER-SystemErrorReporting 事件数: 28				
级别	日期和时间	来源	事件 ID	任务类
❗ 错误	2021/4/22 8:17:41	BugCheck	1001	无
❗ 错误	2021/4/20 13:16:30	BugCheck	1001	无
❗ 错误	2021/4/18 15:25:44	BugCheck	1001	无
❗ 错误	2021/4/18 8:08:23	BugCheck	1001	无
❗ 错误	2021/4/13 16:58:40	BugCheck	1001	无
❗ 错误	2021/4/13 7:45:16	BugCheck	1001	无
❗ 错误	2021/4/6 15:19:35	BugCheck	1001	无
事件 1001, BugCheck				
常规 详细信息				
计算机已经从检测错误后重新启动。检测错误: 0x0000004a (0x00007ff8cd8f0a24, 0x0000000000000002, 0x0000000000000000, 0xffff848530c2f200) 存储的数据保存在: C:\Windows\MEMORY.DMP。报告 ID: aeafe2b7-efa7-473f-843c-7691413c4f49。				

目前怀疑问题原因是: svchost.exe 进程 (承载 DcomLaunch 服务)等待 SearchUI.exe 返回结果, 但超时锁定造成蓝屏现象。

分析过程:

1) Bugcheck 0x0000004a 的解析如下: The IRQL_GT_ZERO_AT_SYSTEM_SERVICE bug check has a value of 0x0000004A. This indicates that a thread is returning to user mode from a system call when its IRQL is still above PASSIVE_LEVEL.

2) 根据 DMP 文件, 可以看到有出问题的子进程是 SearchUI.exe, 线程 ID 为 ffffd28f5d2860c0, 运行在 CPU 3 上。

Process	AttachedProcess	Thread	CID	UserTime
KernelTime ContextSwitches Wait Reason Time State				
System (ffffd28f53296200)	SearchUI.exe (ffffd28f603ca080)	ffffd28f5d2860c0		
4.2b0	0s	172ms	1834 Executive	0s Running on CPU 3

3) 这个 SearchUI.exe 的在月 21 日下午 4:27:33 创建的, 但是等待了 3 小时 59 分钟之后触发了蓝屏。

1: kd> !mex.p ffffd28f603ca080

Name	Address	Ses PID	Act Thrd	Handle	Mods	User
Name	Create Time	Up Time	Z Thrd	Parent		
=====	=====	=====	=====	=====	=====	=====
=====	=====	=====	=====	=====	=====	=====

```
=====
=====
SearchUI.exe ffffd28f603ca080 1 1ce4 (0n7396) 48 0 156 DESKTOP-
DBR1TLD\aaaaa 04/21/2021 04:27:33.041 下午 3h:59:35.958 0 svchost.exe
(DcomLaunch) 50 (0n80)
```

Command Line:

```
"C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.ex
e" -ServerName:CortanaUI.AppXa50dqa5gqv4a428c9y1jjw7m3btvepj.mca
```

4) 而等待的原因, 根据 Bugcheck ID 的解析, 我怀疑是当前线程 ffffd28f5d2860c0 由于中断等级 IRQL 为 0, 所以无法抢占正在 CPU 中运行的其他线程, 导致一直无法执行。而等待反馈的进程 svchost.exe (承载 DcomLaunch 服务)一直等不到反馈结果, 最终造成蓝屏。

```
1: kd> !prcb 3
PRCB for Processor 3 at ffff97000e64a180:
Current IRQL -- 0
Threads-- Current ffffd28f5d2860c0 Next 0000000000000000 Idle
ffff97000e65a180
Processor Index 3 Number (0, 3) GroupSetMember 8
Interrupt Count -- 0049f409
Times -- Dpc 000000fc Interrupt 00000010
Kernel 000e0e1f User 000003e4
```

5) 查看堆栈信息, 怀疑与 dxgmms2!模块有关。

```
1: kd> !mex.t ffffd28f5d2860c0
Process          AttachedProcess      Thread      CID      UserTime
KernelTime ContextSwitches Wait Reason Time State
System (ffffd28f53296200) SearchUI.exe (ffffd28f603ca080) ffffd28f5d2860c0
4.2b0 0s 172ms 1834 Executive 0s Running on CPU 3
```

```
# Child-SP      Return      Call
Site
0 ffff84852e62e988 ffff8034a8b6ef2
nt!KeCopyPage+0x5e open start of
function
```

1 ffff84852e62e990 fffff8034a835bae
nt!MiCopyPage+0x432 open start
of function

2 ffff84852e62eb40 fffff8034a833d91
nt!MiCopyOnWrite+0xcde open start
of function

3 ffff84852e62edb0 fffff8034a8ab9e9
nt!MiValidFault+0x2c1 open start of
function

4 ffff84852e62ee20 fffff8034a8aaa4b
nt!MiUserFault+0x6c9 open start of
function

5 ffff84852e62ef20 fffff8034a8e83cc
nt!MmAccessFault+0x1fb open start
of function

6 ffff84852e62f0c0 fffff8034a8a7b7e
nt!MiFaultInProbeAddress+0xa4 open
start of function

7 ffff84852e62f170 fffff8034a8a6e59
nt!MiProbeAndLockPages+0x3de open
start of function

8 ffff84852e62f2c0 fffff80367583ba8
nt!MmProbeAndLockPages+0x29 open
start of function

9 ffff84852e62f2f0 fffff80367583a79
dxgmms2!VIDMM_MDL_RANGE::Lock+0x6c
open start of function

a ffff84852e62f350 fffff80367580acb
dxgmms2!VIDMM_RECYCLE_HEAP_PHYSICAL_VIEW::LockRange+0xfd
open start of function

b ffff84852e62f3d0 fffff803675809b4
dxgmms2!VIDMM_RECYCLE_RANGE::Lock+0x7b
open start of function

c ffff84852e62f430 fffff803675808fb
dxgmms2!VIDMM_RECYCLE_MULTIRANGE::Lock+0x78
open start of function

d ffff84852e62f490 fffff8036758744a
dxgmms2!VIDMM_RECYCLE_HEAP_MGR::ProbeAndLockAllocation+0x7b
open start of function

```

e ffff84852e62f510 fffff80367587231
dxgmms2!VIDMM_GLOBAL::ProbeAndLockAllocation+0x56
    open start of function
f ffff84852e62f560 fffff80367588dca
dxgmms2!VIDMM_SEGMENT::LockAllocationBackingStore+0xb1
    open start of function
10 ffff84852e62f620 fffff8036758b4bd
dxgmms2!VIDMM_SYSMEM_SEGMENT::CommitResource+0x7a
    open start of function
11 ffff84852e62f660 fffff803675999c6
dxgmms2!VIDMM_GLOBAL::PageInOneAllocation+0x1cd
    open start of function
12 ffff84852e62f770 fffff803675998b7
dxgmms2!VIDMM_GLOBAL::PageInFaultedAllocation+0xaa
    open start of function
13 ffff84852e62f7c0 fffff803675985ec
dxgmms2!VIDMM_GLOBAL::PageInDeviceInternal+0x17f
    open start of function
14 ffff84852e62f830 fffff80367599ab7
dxgmms2!VIDMM_GLOBAL::TryPageInDevice+0x50
    open start of function
15 ffff84852e62f870 fffff803675a5098
dxgmms2!VIDMM_DEVICE::Resume+0x73
    open start of function
16 ffff84852e62f8e0 fffff803675a38a9
dxgmms2!VIDMM_WORKER_THREAD::Run+0x17d8
    open start of function
17 ffff84852e62fae0 fffff8034a920745
dxgmms2!VidMmWorkerThreadProc+0x9
    open start of function
18 ffff84852e62fb10 fffff8034a9c791c
nt!PspSystemThreadStartup+0x55
    open start of function
19 ffff84852e62fb60 0000000000000000
nt!KiStartSystemThread+0x1c
    open start of function

```

This thread has been running on CPU 3 (Pri 15, BasePri 15) for 0s

贾伟 Jia Wei

神州网信技术有限公司

服务支持电话： 400-818-0055

电子邮箱： jiawei@cmgos.com

C&M Information Technologies Co., Ltd.

11F, Block C North Building, Raycom InfoTech Park, Beijing

mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人: 城市猎人 <423689835@qq.com>

发送时间: 2021 年 5 月 19 日 15:32

收件人: Jia Wei <jiawei@cmgos.com>

主题: 回复: 回复: 回复: [案例号: CAS-04004-N2H1M1] % 经销商南宁市纪云科技有限公司反馈客户来宾市住房和城乡建设局蓝屏问题 % 初次响应 CMIT:0001184

刚打电话给客户，客户说没有蓝屏了，感谢

---原始邮件---

发件人: "Jia Wei" <jiawei@cmgos.com>

发送时间: 2021 年 5 月 19 日(周三) 下午 2:25

收件人: "城市猎人" <423689835@qq.com>;

抄送: "Case_Notification" <Case_Notification@cmgos.com>;

主题: 回复: 回复: [案例号: CAS-04004-N2H1M1] % 经销商南宁市纪云科技有限公司反馈客户来宾市住房和城乡建设局蓝屏问题 % 初次响应 CMIT:0001184

覃先生，您好：

下一步建议：

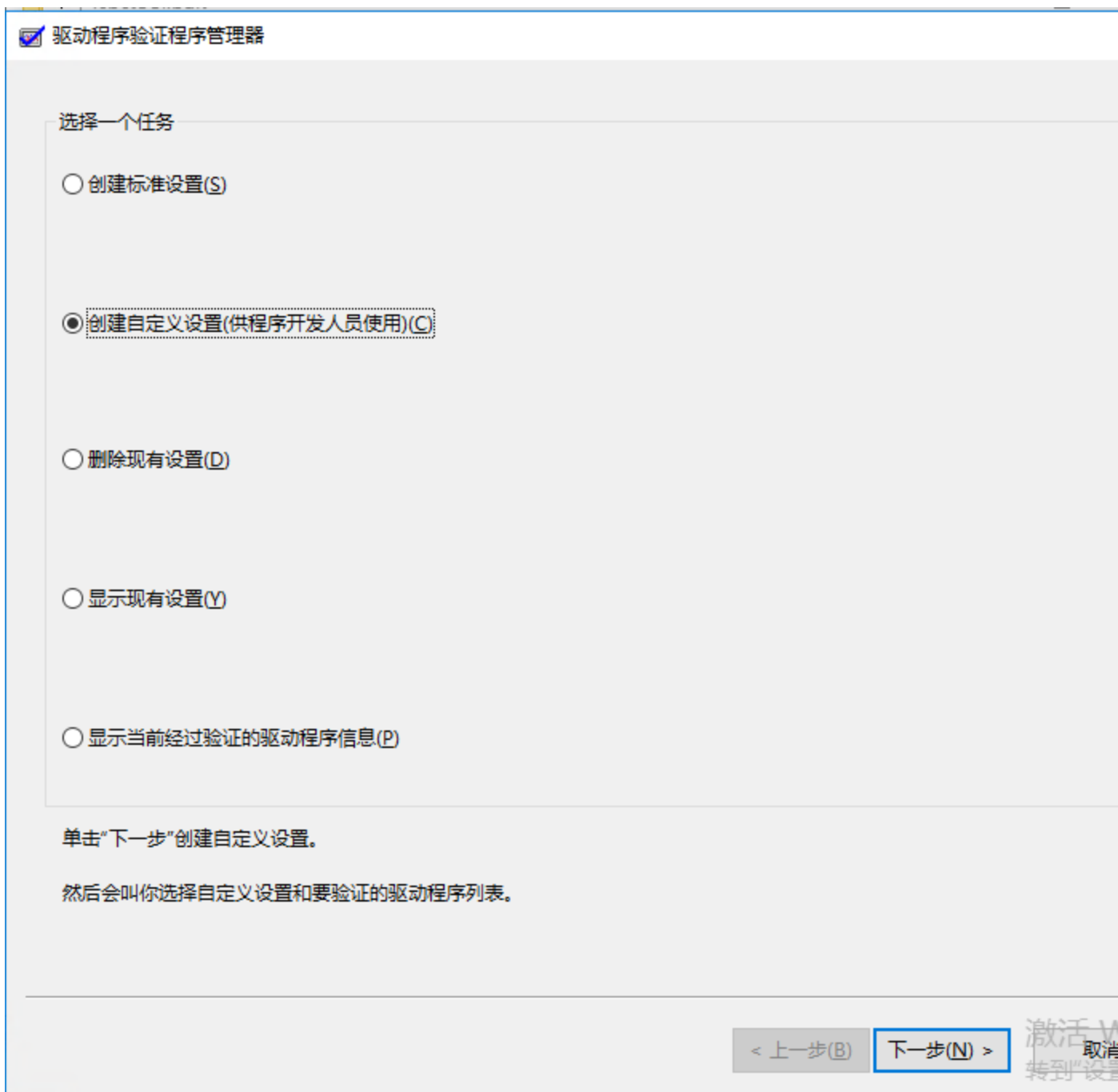
目前查看您的及其同时按照了 360 和 QQ 相关软件（可能是防病毒或管理软件），由于查看到蓝屏时运行 360 公司的程序且很多问题都是由此导致的，所以建议卸载这两个软件之后确认问题是否复现。

日志收集：


如果需要再进一步确认是哪个驱动导致问题原因，需要按照如下配置之后收集 dump 文件。

1. 开启 driver verify

- 1) 右键开始菜单点击运行，输入“**verifier.exe**” 点击确认。
- 2) 选择“**创建自定义设置**” 然后点下一步。



3) 勾选 “ I/O 验证 ” 和 “ 杂项检查 ” 点击 “ 下一步 ”

 驱动程序验证程序管理器

从这个完整列表选择单个设置

已启用了吗?	测试类型	标志类型	
<input type="checkbox"/>	特殊池	标准	
<input type="checkbox"/>	强制 IRQL 检查	标准	
<input type="checkbox"/>	随机低资源模拟	其他	
<input type="checkbox"/>	池跟踪	标准	
<input checked="" type="checkbox"/>	I/O 验证	标准	
<input type="checkbox"/>	死锁检测	标准	
<input type="checkbox"/>	DMA 检查	标准	
<input type="checkbox"/>	安全性检查	标准	
<input type="checkbox"/>	强制挂起 I/O 请求 (*)	其他	
<input type="checkbox"/>	IRP 日志 (*)	其他	
<input checked="" type="checkbox"/>	杂项检查	标准	
<input type="checkbox"/>	堆栈的固定 MDL 检查 (*)	其他	
<input type="checkbox"/>	驱动程序的固定 MDL 检查 (*)	其他	
<input type="checkbox"/>	Power 框架延迟模糊处理	其他	
<input type="checkbox"/>	端口/微型端口接口检查	其他	
<input type="checkbox"/>	DDI 兼容性检查	标准	
<input type="checkbox"/>	系统低资源模拟	其他	
<input type="checkbox"/>	DDI 兼容性检查(额外)	其他	

在选择要创建的设置后，单击“下一步”。

然后，将要求你选择要验证的驱动程序。

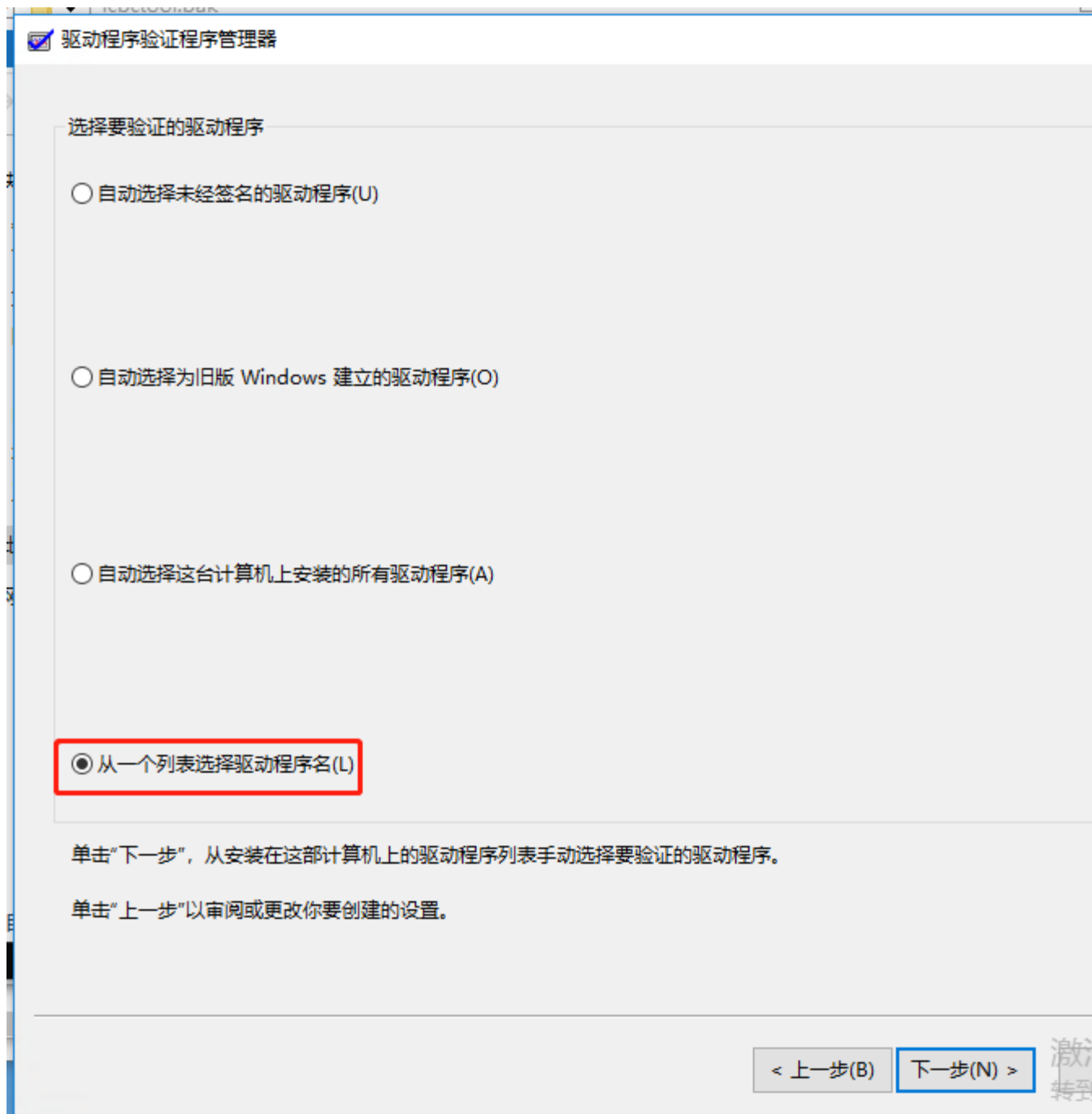
标有 (*) 的标记还要求启用 I/O 验证(第 4 位)。

< 上一步(B)

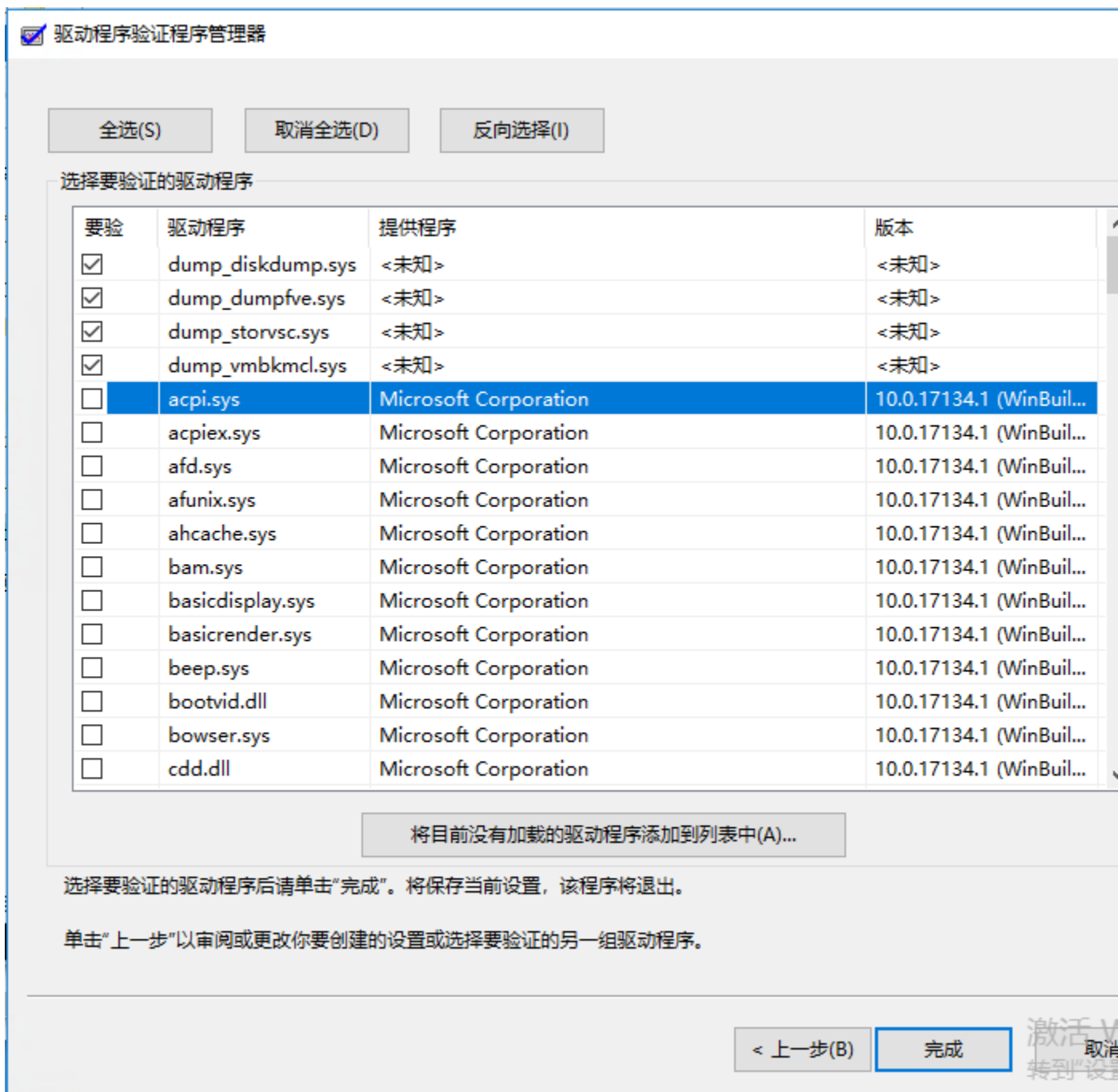
下一步(N) >

激活 V
转到“设置”

4) 选择“从一个列表选择驱动程序名”然后点击下一步。



- 3) 点击“提供程序”将驱动按照提供程序厂商进行排列，然后选择所有提供程序为非微软的驱动
参考如下示例：



- 4) 重启系统，计算机启动并登录后，使用以下命令验证是否已针对所选选项验证以上驱动程序列表（以管理员权限打开 cmd）：**verifier**
/querysettings
【X】代表启用成功，【 】代表未启用

验证程序标志: 0x00000810

标准标志:

```
[ ] 0x00000001 特殊池。  
[ ] 0x00000002 强制 IRQL 检查。  
[ ] 0x00000008 池跟踪。  
[X] 0x00000010 I/O 验证。  
[ ] 0x00000020 死锁检测。  
[ ] 0x00000080 DMA 检查。  
[ ] 0x00000100 安全检查。  
[X] 0x00000800 杂项检查。  
[ ] 0x00020000 DDI 兼容性检查。
```

其他标志:

```
[ ] 0x00000004 随机低资源模拟。  
[ ] 0x00000200 强制挂起 I/O 请求。  
[ ] 0x00000400 IRP 日志记录。  
[ ] 0x00002000 堆栈的固定 MDL 检查。  
[ ] 0x00004000 驱动程序的固定 MDL 检查。  
[ ] 0x00008000 Power 框架延迟模糊处理。  
[ ] 0x00010000 端口/微型端口接口检查。  
[ ] 0x00040000 系统低资源模拟。  
[ ] 0x00080000 DDI 兼容性检查(额外)。  
[ ] 0x00200000 NDIS/WLAN 验证。  
[ ] 0x00800000 内核同步延迟模糊处理。  
[ ] 0x01000000 VM 开关验证。  
[ ] 0x02000000 代码完整性检查。
```

[X] 指示标志已启用。

引导模式:

Persistent

- 5) 正常运行系统。一旦驱动程序验证程序检测到任何经过验证的驱动程序违规, 它将使系统崩溃。收集最新的 Dump 文件和事件日志
- 6) 解决问题后, 请使用以下命令禁用驱动程序验证程序: **verifier /reset** 重新启动机器。

贾伟 Jia Wei

神州网信技术有限公司

服务支持电话： 400-818-0055

电子邮箱： jiawei@cmgos.com

C&M Information Technologies Co., Ltd.

11F, Block C North Building, Raycom InfoTech Park, Beijing

mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人：Jia Wei

发送时间：2021 年 5 月 12 日 13:44

收件人：'城市猎人' <423689835@qq.com>

抄送：Case_Notification <Case_Notification@cmgos.com>

主题：回复：回复：[案例号：CAS-04004-N2H1M1] % 经销商南宁市纪云科技有限公司反馈客户来宾市住房和城乡建设局蓝屏问题 % 初次响应 CMIT:0001184

覃先生，您好：

来信是想咨询当前案件进展状况。

如果针对当前案件还有需要我们帮助的地方，欢迎随时联系我们。

贾伟 Jia Wei

神州网信技术有限公司

服务支持电话： 400-818-0055

电子邮箱： jiawei@cmgos.com

C&M Information Technologies Co., Ltd.

11F, Block C North Building, Raycom InfoTech Park, Beijing
mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人: Jia Wei

发送时间: 2021 年 5 月 8 日 9:52

收件人: '城市猎人' <423689835@qq.com>

抄送: Case_Notification <Case_Notification@cmgos.com>

主题: 回复: 回复: [案例号: CAS-04004-N2H1M1] % 经销商南宁市纪云科技有限公司反馈客户来宾市住房和城乡建设局蓝屏问题 % 初次响应 CMIT:0001184

覃先生, 您好

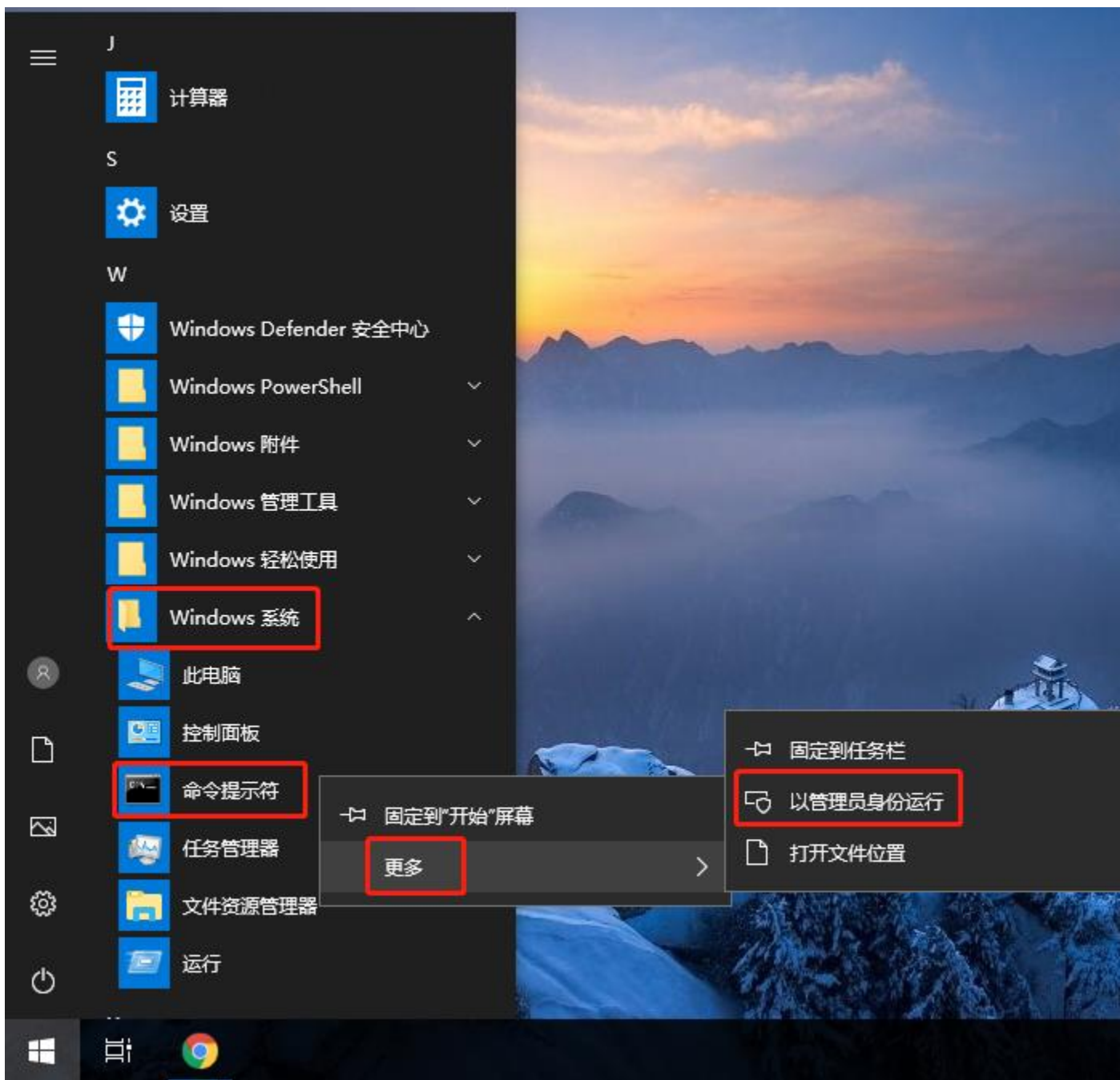
正如电话沟通, 如果客户更换显卡驱动后未复现蓝屏问题, 您可以回复此邮件; 如果仍有问题, 您到现场后可以收集如下日志文件回传, 以便我们进一步分析问题。

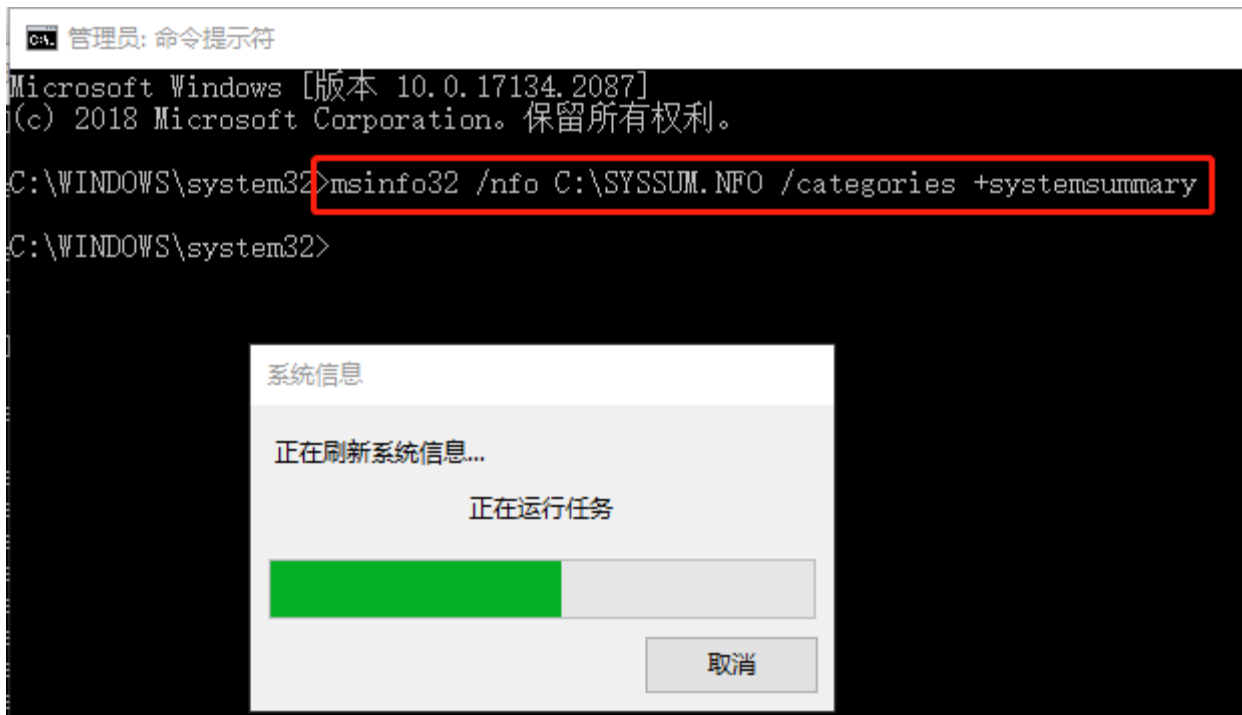
1) 如果之前已按要求配置完成, 之后只要出现蓝屏, 就会在 C:\Windows 下自动生成 MEMORY.DMP 文件, 将其压缩后上传;

2) 以管理员身份运行命令提示符 (cmd), 运行如下命令, 并在收集

C:\SYSSUM.NFO 压缩上传;

msinfo32 /nfo C:\SYSSUM.NFO /categories +systemsummary





3) 工具收集

- 1 下载附件 zip 文件并解压到本地磁盘。之后双击运行 exe 文件，同意隐私声明后，按照下图勾选系统日志，组策略信息、网络信息、软件信息，系统进程、已安装补丁，点击收集。



- 1 收集完毕后将在当前用户桌面生产 CMGE_Log。点击确定，将直接打开文件夹并定为压缩文件。
- 1 将日志文件上传。

日志上传与下载

Filezilla client 端下载 URL: <https://filezilla-project.org/download.php?type=client>

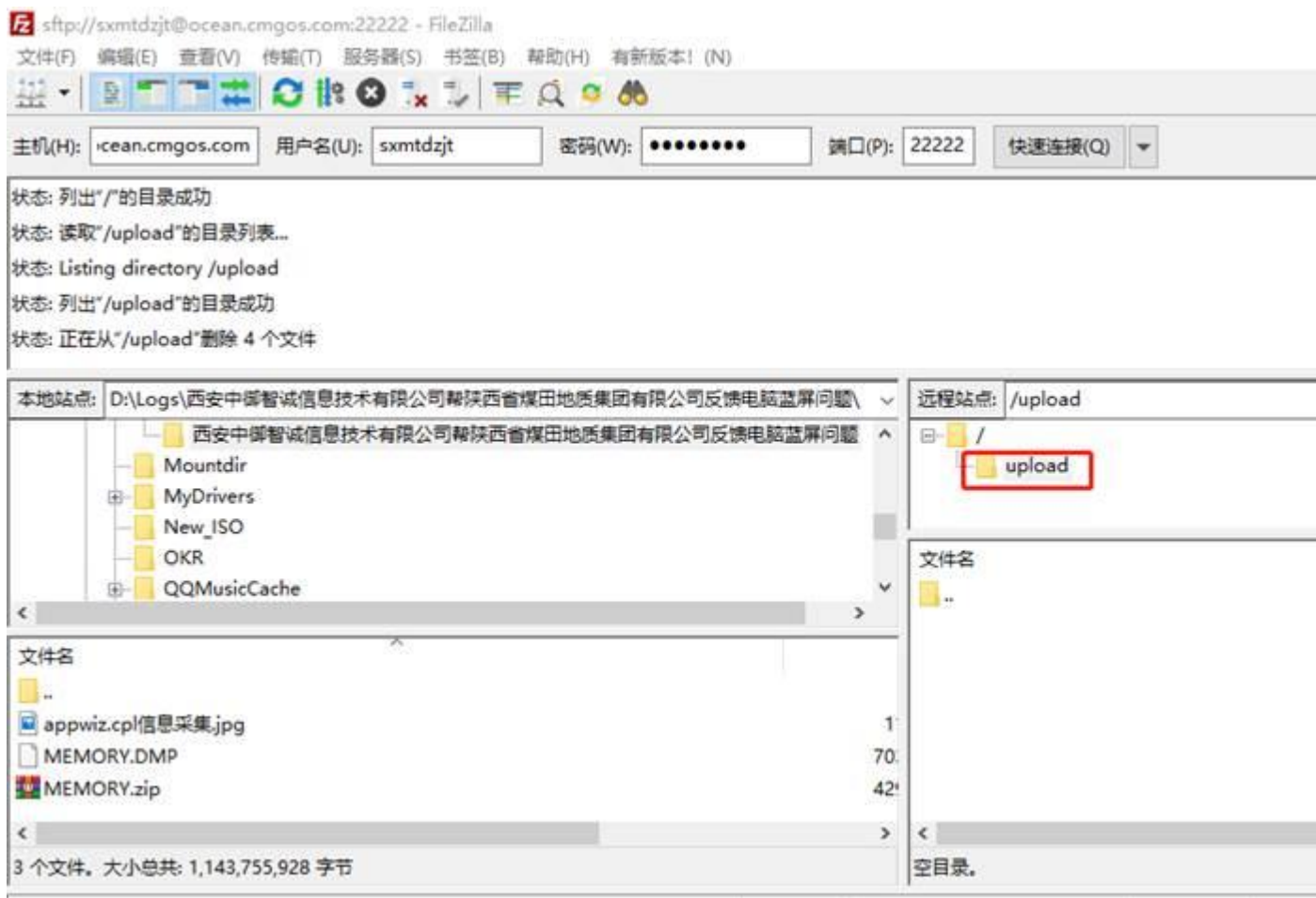
主机: sftp://ocean.cmgos.com

用户名为: lbszjj

密码: 1234.asd

端口: 22222

登陆后选择 Upload 文件夹上传。



贾伟 Jia Wei
神州网信技术有限公司
服务支持电话: 400-818-0055
电子邮箱: jiawei@cmgos.com

C&M Information Technologies Co., Ltd.
11F, Block C North Building, Raycom InfoTech Park, Beijing
mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人: Jia Wei
发送时间: 2021 年 5 月 6 日 10:16
收件人: '城市猎人' <423689835@qq.com>
抄送: Case_Notification <Case_Notification@cmgos.com>

主题：回复：[案例号：CAS-04004-N2H1M1] % 经销商南宁市纪云科技有限公司
反馈客户来宾市住房和城乡建设局蓝屏问题 % 初次响应 CMIT:0001184

您好，

更换显卡驱动程序之后，用户蓝屏问题是否得到缓解？如果有进展您可以回复此邮件。

贾伟 Jia Wei
神州网信技术有限公司
服务支持电话： 400-818-0055
电子邮箱： jiawei@cmgos.com

C&M Information Technologies Co., Ltd.
11F, Block C North Building, Raycom InfoTech Park, Beijing
mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人：Jia Wei
发送时间：2021 年 4 月 28 日 13:26
收件人：‘城市猎人’ <423689835@qq.com>
抄送：Case_Notification <Case_Notification@cmgos.com>
主题：回复：回复：回复：回复：[案例号：CAS-04004-N2H1M1] % 经销商南宁市纪云科技有限公司反馈客户来宾市住房和城乡建设局蓝屏问题 % 初次响应
CMIT:0001184

您好，

我们会在对日志文件进行查看，另外如果再次出现蓝屏问题，可以再回传新生成的 dump 文件。

贾伟 Jia Wei
神州网信技术有限公司
服务支持电话： 400-818-0055
电子邮箱： jiawei@cmgos.com

C&M Information Technologies Co., Ltd.
11F, Block C North Building, Raycom InfoTech Park, Beijing

mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人: 城市猎人 <423689835@qq.com>

发送时间: 2021 年 4 月 28 日 10:14

收件人: Jia Wei <jiawei@cmgos.com>

主题: 回复: 回复: 回复: [案例号: CAS-04004-N2H1M1] % 经销商南宁市纪云科技有限公司反馈客户来宾市住房和城乡建设局蓝屏问题 % 初次响应
CMIT:0001184

刚才说的 22 版本驱动另外一台电脑也蓝屏过,

---原始邮件---

发件人: "Jia Wei" <jiawei@cmgos.com>

发送时间: 2021 年 4 月 26 日 (周一) 下午 2:52

收件人: "城市猎人" <423689835@qq.com>;

抄送: "Case_Notification" <Case_Notification@cmgos.com>;

主题: 回复: 回复: [案例号: CAS-04004-N2H1M1] % 经销商南宁市纪云科技有限公司反馈客户来宾市住房和城乡建设局蓝屏问题 % 初次响应 CMIT:0001184

覃先生, 您好:

来信是想咨询当前案件进展状况。

如果针对当前案件还有需要我们帮助的地方, 欢迎随时联系我们。

贾伟 Jia Wei

神州网信技术有限公司

服务支持电话: 400-818-0055

电子邮箱: jiawei@cmgos.com

C&M Information Technologies Co., Ltd.

11F, Block C North Building, Raycom InfoTech Park, Beijing

mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人: Jia Wei

发送时间: 2021 年 4 月 23 日 15:26

收件人: '城市猎人' <423689835@qq.com>

抄送: Case_Notification <Case_Notification@cmgos.com>

主题: 回复: [案例号: CAS-04004-N2H1M1] % 经销商南宁市纪云科技有限公司
反馈客户来宾市住房和城乡建设局蓝屏问题 % 初次响应 CMIT:0001184

您好,

那只能安装 1903 的显卡驱动先观察一下。注意对比安装前后的驱动版本信息。

如果仍有问题, 建议:

- 1) 回退操作系统初始显卡驱动, 观察问题是否复现;
- 2) 查看其他未出现蓝屏的显卡驱动, 使用此驱动安装。

贾伟 Jia Wei

神州网信技术有限公司

服务支持电话: 400-818-0055

电子邮箱: jiawei@cmgos.com

C&M Information Technologies Co., Ltd.

11F, Block C North Building, Raycom InfoTech Park, Beijing

mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人: 城市猎人 <423689835@qq.com>

发送时间: 2021 年 4 月 23 日 15:06

收件人: Jia Wei <jiawei@cmgos.com>

主题: 回复: 回复: 回复: [案例号: CAS-04004-N2H1M1] % 经销商南宁市纪云
科技有限公司反馈客户来宾市住房和城乡建设局蓝屏问题 % 初次响应
CMIT:0001184

联想回复说没有 1809 驱动

---原始邮件---

发件人: "Jia Wei"<jiawei@cmgos.com>
发送时间: 2021 年 4 月 23 日(周五) 下午 2:12
收件人: "城市猎人"<423689835@qq.com>;
抄送:
"624687084@qq.com"<624687084@qq.com>;"Case_Notification"<Case_Notification@cmgos.com>;
主题: 回复: 回复: [案例号: CAS-04004-N2H1M1] % 经销商南宁市纪云科技有限公司反馈客户来宾市住房和城乡建设局蓝屏问题 % 初次响应 CMIT:0001184

覃先生, 您好

案例分析:

- 1 目前看到系统事件日志有大量蓝屏 Bugcheck 报错, 本次的报错为 0x0000004a。
其余多次各不相同, 例如: 0x0000007e、0x00000051、0x000000ef 等。
- 1 蓝屏问题触发时, 每次会生成一个 MEMORY.DMP 文件。当前只针对本次生成的 Bugcheck 为 0x0000004a 的问题进行分析, 分析结果不代表其他蓝屏问题的原因。

System_20 事件数: 15,293

已筛选: 日志: file://D:\Logs\CAS-04004-N2H1M1\20210422_082451\EventLog\System.evtx; 级别: 关键, 错误, 警告; 来源: Microsoft-Windows-WER-SystemErrorReporting。事件数: 28

级别	日期和时间	来源	事件 ID	任务类
错误	2021/4/22 8:17:41	BugCheck	1001	无
错误	2021/4/20 13:16:30	BugCheck	1001	无
错误	2021/4/18 15:25:44	BugCheck	1001	无
错误	2021/4/18 8:08:23	BugCheck	1001	无
错误	2021/4/13 16:58:40	BugCheck	1001	无
错误	2021/4/13 7:45:16	BugCheck	1001	无
错误	2021/4/6 15:19:35	BugCheck	1001	无

事件 1001, BugCheck

常规 详细信息

计算机已经从检测错误后重新启动。检测错误: 0x0000004a (0x00007ff8cd8f0a24, 0x0000000000000002, 0x0000000000000000, 0xffff848530c2f000) 存储的数据保存在: C:\Windows\MEMORY.DMP。报告 ID: aeafe2b7-efa7-473f-843c-7691413c4f49。

目前怀疑问题原因是：svchost.exe 进程（承载 DcomLaunch 服务）等待 SearchUI.exe 返回结果，但超时锁定造成蓝屏现象。

分析过程：

1) Bugcheck 0x0000004a 的解析如下：The IRQL_GT_ZERO_AT_SYSTEM_SERVICE bug check has a value of 0x0000004A. This indicates that a thread is returning to user mode from a system call when its IRQL is still above PASSIVE_LEVEL.

2) 根据 DMP 文件，可以看到有出问题的子进程是 SearchUI.exe，线程 ID 为 fffffd28f5d2860c0，运行在 CPU 3 上。

Process		AttachedProcess	
Thread		CID	UserTime KernelTime
ContextSwitches Wait Reason Time State			
System (fffffd28f53296200) SearchUI.exe (fffffd28f603ca080)			
fffffd28f5d2860c0			
4. 2b0	0s	172ms	1834
Executive	0s Running on CPU 3		

3) 这个 SearchUI.exe 的在月 21 日下午 4:27:33 创建的，但是等待了 3 小时 59 分钟之后触发了蓝屏。

1: kd> !mex.p fffffd28f603ca080

Name	Address	Ses	PID	Act
Thrd Handle	Mods	User	Name	Create
Time		Up	Time	Z Thrd
Parent				

```
=====
=====
=====
```

```
SearchUI.exe fffffd28f603ca080 1 1ce4
(0n7396) 48 0 156 DESKTOP-DBR1TLD\aaaaa 04/21/2021
04:27:33.041 下午 3h:59:35.958 0 svchost.exe (DcomLaunch) 50
(0n80)
```

Command Line:

```
"C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.
exe" -ServerName:CortanaUI.AppXa50dqa5gqv4a428c9y1jjw7m3btvepj.mca
```

4) 而等待的原因, 根据 Bugcheck ID 的解析, 我怀疑是当前线程 fffffd28f5d2860c0 由于中断等级 IRQL 为 0, 所以无法抢占正在 CPU 中运行的其他线程, 导致一直无法执行。而等待反馈的进程 svchost.exe (承载 DcomLaunch 服务) 一直等不到反馈结果, 最终造成蓝屏。

```
1: kd> !prcb 3
```

```
PRCB for Processor 3 at ffff97000e64a180:
```

```
Current IRQL -- 0
```

```
Threads-- Current fffffd28f5d2860c0 Next 0000000000000000 Idle
ffff97000e65a180
```

```
Processor Index 3 Number (0, 3) GroupSetMember 8
```

```
Interrupt Count -- 0049f409
```

```
Times -- Dpc 000000fc Interrupt 00000010
```

```
Kernel 000e0e1f User 000003e4
```


5) 查看堆栈信息, 怀疑与 dxgmms2!模块有关。

1: kd> !mex.t fffffd28f5d2860c0

Process	Thread	AttachedProcess	CID	UserTime	KernelTime
ContextSwitches	Wait Reason	Time	State		
System (fffffd28f53296200)	SearchUI.exe (fffffd28f603ca080)				
fffffd28f5d2860c0					
4.2b0	0s	172ms		1834	
Executive	0s Running on CPU 3				

# Child-SP	Return	Call
Site		

Source

0 fffff84852e62e988 fffff8034a8b6ef2
nt!KeCopyPage+0x5e

open start of function

1 fffff84852e62e990 fffff8034a835bae
nt!MiCopyPage+0x432

open start of function

2 fffff84852e62eb40 fffff8034a833d91
nt!MiCopyOnWrite+0xcde

open start of function

3 fffff84852e62edb0 fffff8034a8ab9e9
nt!MiValidFault+0x2c1

open start of function

4 fffff84852e62ee20 fffff8034a8aaa4b
nt!MiUserFault+0x6c9

open start of function

5 ffff84852e62ef20 fffff8034a8e83cc
nt!MmAccessFault+0x1fb

open start of function

6 ffff84852e62f0c0 fffff8034a8a7b7e
nt!MiFaultInProbeAddress+0xa4

open start of function

7 ffff84852e62f170 fffff8034a8a6e59
nt!MiProbeAndLockPages+0x3de

open start of function

8 ffff84852e62f2c0 fffff80367583ba8
nt!MmProbeAndLockPages+0x29

open start of function

9 ffff84852e62f2f0 fffff80367583a79
dxgmms2!VIDMM_MDL_RANGE::Lock+0x6c

open start of function

a ffff84852e62f350 fffff80367580acb
dxgmms2!VIDMM_RECYCLE_HEAP_PHYSICAL_VIEW::LockRange+0xfd

open start of

function

b ffff84852e62f3d0 fffff803675809b4
dxgmms2!VIDMM_RECYCLE_RANGE::Lock+0x7b

open start of function

c ffff84852e62f430 fffff803675808fb
dxgmms2!VIDMM_RECYCLE_MULTIRANGE::Lock+0x78

o

pen start of function

d	ffff84852e62f490	fffff8036758744a	
	dxgmms2!VIDMM_RECYCLE_HEAP_MGR::ProbeAndLockAllocation+0x7b		
			open start of
	function		
e	ffff84852e62f510	fffff80367587231	
	dxgmms2!VIDMM_GLOBAL::ProbeAndLockAllocation+0x56		
			open
	start of function		
f	ffff84852e62f560	fffff80367588dca	
	dxgmms2!VIDMM_SEGMENT::LockAllocationBackingStore+0xb1		
			open start
	of function		
10	ffff84852e62f620	fffff8036758b4bd	
	dxgmms2!VIDMM_SYSMEM_SEGMENT::CommitResource+0x7a		
			open
	start of function		
11	ffff84852e62f660	fffff803675999c6	
	dxgmms2!VIDMM_GLOBAL::PageInOneAllocation+0x1cd		
			open
	start of function		
12	ffff84852e62f770	fffff803675998b7	
	dxgmms2!VIDMM_GLOBAL::PageInFaultedAllocation+0xaa		
			open start
	of function		
13	ffff84852e62f7c0	fffff803675985ec	
	dxgmms2!VIDMM_GLOBAL::PageInDeviceInternal+0x17f		
			open
	start of function		
14	ffff84852e62f830	fffff80367599ab7	
	dxgmms2!VIDMM_GLOBAL::TryPageInDevice+0x50		
	open start of function		
15	ffff84852e62f870	fffff803675a5098	
	dxgmms2!VIDMM_DEVICE::Resume+0x73		

open start of function

16 ffff84852e62f8e0 fffff803675a38a9
dxgmmms2!VIDMM_WORKER_THREAD::Run+0x17d8

open start of function

17 ffff84852e62fae0 fffff8034a920745
dxgmmms2!VidMmWorkerThreadProc+0x9

open start of function

18 ffff84852e62fb10 fffff8034a9c791c
nt!PspSystemThreadStartup+0x55

open start of function

19 ffff84852e62fb60 0000000000000000
nt!KiStartSystemThread+0x1c

open start of function

This thread has been running on CPU 3 (Pri 15, BasePri 15) for 0s

建议操作：

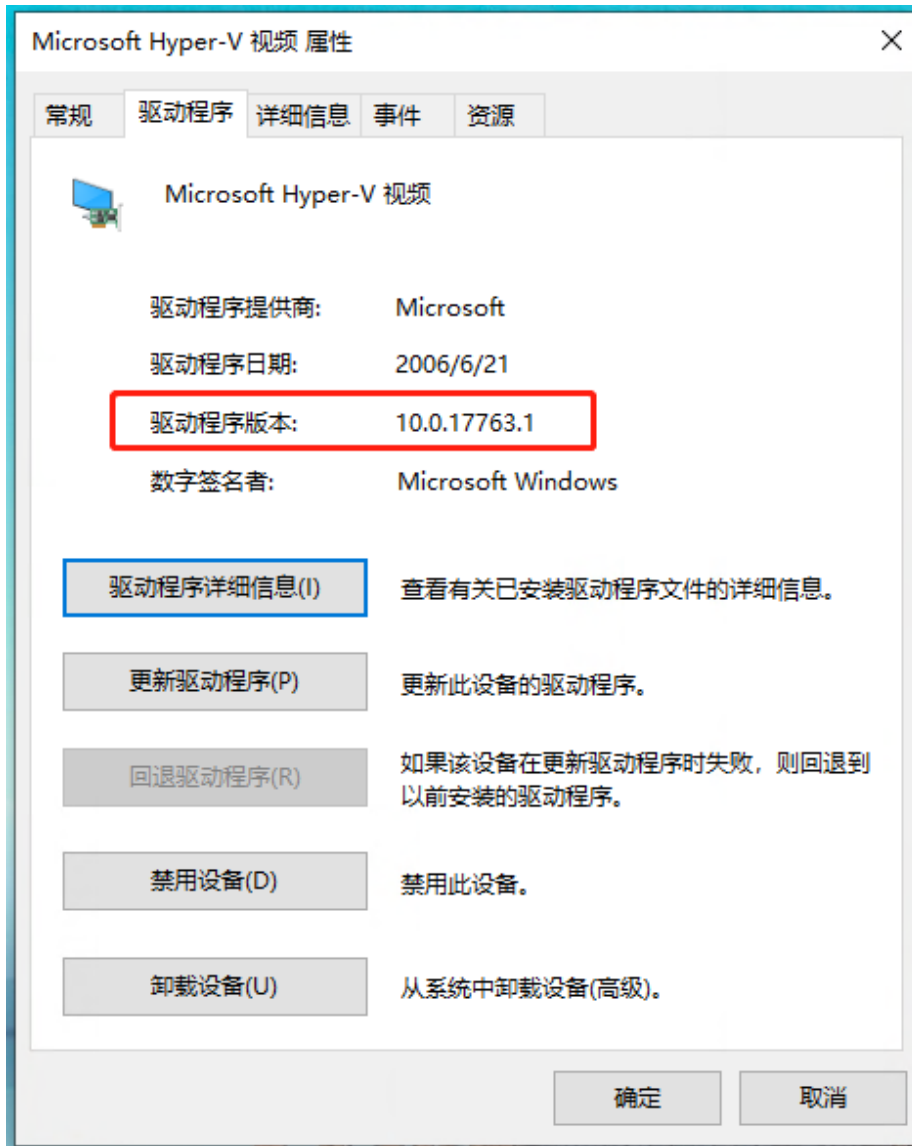
dxgmmms2.sys 文件是 Windows 系统驱动程序文件，它与计算机的图形呈现功能相关
联。

一、重新安装当前计算机的网卡驱动。

1) 右键单击开始按钮，选择设备管理器



2) 找到显示适配器，选择当前的物理显卡，右键点击选择属性，在驱动程序标签页，将此窗口全部截图保留。



3) 确认当前计算机的品牌和型号, 务必从官方网站下载、安装适用于 Windows 10 64 位、最新的对应品牌的驱动程序。我从系统信息看到的是 LENOVO 11BRA0U1CD。请再次确认。

<https://think.lenovo.com.cn/support/driver/newdriversdownlist.aspx?categoryid=3112948&CODENAME=&SearchType=1&wherePage=1&SearchNodeCC=&needmt=11BRA0U1CD>

⊖ 显卡 (3)

驱动名称	版本	系统
NVIDIA 显卡驱动程序(Windows 10 64-bit 1903 及之后...	26.21.14.4	Windows 10
AMD 显卡驱动程序(Windows 10 64-bit 1903 及之后版本)	26.20.1405	Windows 10
Intel 显卡驱动程序(Windows 10 64-bit 1903 及之后版...	27.20.100.	Windows 10

注意：我看到此设备 ThinkCentre E76p 的显卡驱动都标注了（Windows 10 64-bit 1903 及之后版本），而 CMGE V2020-L 是基于 Windows 10 企业版 G 1809 版本进行定制开发的，所以需要您与联想售后电话沟通，确认是否有 1809 版本的显卡驱动。

***供应商信息：**

400-810-6666 周一至周日 9:00-18:00 Think 产品服务热线

400-100-6000 ThinkPad 笔记本、ThinkPad

4) 按照第 2 步，确认驱动程序版本是否已经更改。

如果上述操作未能缓解蓝屏问题，请回复此邮件。

贾伟 Jia Wei

神州网信技术有限公司

服务支持电话： 400-818-0055

电子邮箱： jiawei@cmgos.com

C&M Information Technologies Co., Ltd.

11F, Block C North Building, Raycom InfoTech Park, Beijing

mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人: Jia Wei

发送时间: 2021 年 4 月 22 日 14:14

收件人: '城市猎人' <423689835@qq.com>

抄送: '624687084@qq.com' <624687084@qq.com>; Case_Notification
<Case_Notification@cmgos.com>

主题: 回复: [案例号: CAS-04004-N2H1M1] % 经销商南宁市纪云科技有限公司
反馈客户来宾市住房和城乡建设局蓝屏问题 % 初次响应 CMIT:0001184

覃先生, 您好

您上传的日志文件已经完成, 我正在下载日志文件。

贾伟 Jia Wei

神州网信技术有限公司

服务支持电话: 400-818-0055

电子邮箱: jiawei@cmgos.com

C&M Information Technologies Co., Ltd.

11F, Block C North Building, Raycom InfoTech Park, Beijing

mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人: Jia Wei

发送时间: 2021 年 4 月 22 日 10:44

收件人: '城市猎人' <423689835@qq.com>

抄送: '624687084@qq.com' <624687084@qq.com>; Case_Notification
<Case_Notification@cmgos.com>

主题: 回复: 回复: 回复: 回复: [案例号: CAS-04004-N2H1M1] % 经销商南宁

市纪云科技有限公司反馈客户来宾市住房和城乡建设局蓝屏问题 % 初次响应
CMIT:0001184

好的覃先生，

我会观察如果上传完毕我会第一时间下载，并发邮件告知您。

贾伟 Jia Wei
神州网信技术有限公司
服务支持电话： 400-818-0055
电子邮箱： jiawei@cmgos.com

C&M Information Technologies Co., Ltd.
11F, Block C North Building, Raycom InfoTech Park, Beijing
mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人：城市猎人 <423689835@qq.com>
发送时间：2021 年 4 月 22 日 10:19
收件人：Jia Wei <jiawei@cmgos.com>
主题：回复：回复：回复：[案例号：CAS-04004-N2H1M1] % 经销商南宁市纪云科技有限公司反馈客户来宾市住房和城乡建设局蓝屏问题 % 初次响应
CMIT:0001184

你收到了也回复我下，因为太久了，我就不在哪里等了，

---原始邮件---

发件人："Jia Wei"<jiawei@cmgos.com>
发送时间：2021 年 4 月 22 日(周四) 上午 9:22
收件人："城市猎人"<423689835@qq.com>;
主题：回复：回复：[案例号：CAS-04004-N2H1M1] % 经销商南宁市纪云科技有限公司反馈客户来宾市住房和城乡建设局蓝屏问题 % 初次响应 CMIT:0001184

您好，

不好意思，目前公司还没有微信支持方式。日志文件需要您实验 sftp 服务器上
传。

上传速度受到您本地网络限制影响，如果比较慢您可以尝试使用手机热点或其他网络，或者找到网络管理员对端口上传速率进行重新设定。

贾伟 Jia Wei

神州网信技术有限公司

服务支持电话： 400-818-0055

电子邮箱： jiawei@cmgos.com

C&M Information Technologies Co., Ltd.

11F, Block C North Building, Raycom InfoTech Park, Beijing

mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人：城市猎人 <423689835@qq.com>

发送时间：2021 年 4 月 22 日 9:17

收件人：Jia Wei <jiawei@cmgos.com>

主题：回复：[案例号：CAS-04004-N2H1M1] % 经销商南宁市纪云科技有限公司
反馈客户来宾市住房和城乡建设局蓝屏问题 % 初次响应 CMIT:0001184

可以加微信传给你嘛。这样用你们的软件太慢了

---原始邮件---

发件人：“Jia Wei”<jiawei@cmgos.com>

发送时间：2021 年 4 月 22 日(周四) 上午 8:45

收件人: "城市猎人"<423689835@qq.com>;

主题: Re: [案例号: CAS-04004-N2H1M1] % 经销商南宁市纪云科技有限公司反馈客户来宾市住房和城乡建设局蓝屏问题 % 初次响应 CMIT:0001184

你好, 我 9 点到办公室。到了给您打电话。

发自我的 iPhone

在 2021 年 4 月 22 日, 08:42, 城市猎人 <423689835@qq.com> 写道:

几点上班, 着急找你

---原始邮件---

发件人: "Jia Wei"<jiawei@cmgos.com>

发送时间: 2021 年 4 月 19 日(周一) 中午 1:35

收件人:

"624687084"<624687084@qq.com>; "423689835@qq.com"<423689835@qq.com>;

抄送: "Case_Notification"<Case_Notification@cmgos.com>;

主题: 回复: 回复: 回复: [案例号: CAS-04004-N2H1M1] % 经销商南宁市纪云科技有限公司反馈客户来宾市住房和城乡建设局蓝屏问题 % 初次响应 CMIT:0001184

好的,

如果有疑问, 或者需要我们协助, 可回复此邮件。

我们可以电话进行沟通。

贾伟 Jia Wei

神州网信技术有限公司

服务支持电话： 400-818-0055

电子邮箱： jiawei@cmgos.com

C&M Information Technologies Co., Ltd.

11F, Block C North Building, Raycom InfoTech Park, Beijing

mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人：624687084 <624687084@qq.com>

发送时间：2021 年 4 月 15 日 13:37

收件人：Jia Wei <jiawei@cmgos.com>

主题：回复：回复：回复：[案例号：CAS-04004-N2H1M1] % 经销商南宁市纪云科技有限公司反馈客户来宾市住房和城乡建设局蓝屏问题 % 初次响应
CMIT:0001184

三月三广西这边放假的

原始邮件

发件人：“Jia Wei” <jiawei@cmgos.com>;

发送时间： 2021 年 4 月 15 日(星期四) 上午 10:53

收件人： “城市猎人”<423689835@qq.com>;

抄

送： “Case_Notification”<Case_Notification@cmgos.com>;“624687084”<624687084@qq.com>;

主题： 回复： 回复： 回复： [案例号： CAS-04004-N2H1M1] % 经销商南宁市纪云科技有限公司反馈客户来宾市住房和城乡建设局蓝屏问题 % 初次响应
CMIT:0001184

覃先生，您好！

来信是想咨询当前案件进展状况。

如果针对当前案件还有需要我们帮助的地方，欢迎随时联系我们。

贾伟 Jia Wei

神州网信技术有限公司

服务支持电话： 400-818-0055

电子邮箱： jiawei@cmgos.com

C&M Information Technologies Co., Ltd.

11F, Block C North Building, Raycom InfoTech Park, Beijing

mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人: Jia Wei

发送时间: 2021 年 4 月 13 日 16:57

收件人: '城市猎人' <423689835@qq.com>

抄送: Case_Notification <Case_Notification@cmgos.com>; "'624687084"' <624687084@qq.com>

主题: 回复: 回复: 回复: [案例号: CAS-04004-N2H1M1] % 经销商南宁市纪云科技有限公司反馈客户来宾市住房和城乡建设局蓝屏问题 % 初次响应
CMIT:0001184

您好,

如果之前已按要求配置完成,之后只要触发蓝屏,就会在 C:\Windows 下自动生成 MEMORY.DMP 文件,大小应该与您内存大小类似,例如 8G 内存,那么 MEMORY.DMP 文件应该也大概 8G 左右。压缩之后会更便于上传。

您可以看下,现在有没有此文件。

如果您还有问题,可以回复方便的时间电话沟通一下。

贾伟 Jia Wei

神州网信技术有限公司

服务支持电话: 400-818-0055

电子邮箱: jiawei@cmgos.com

C&M Information Technologies Co., Ltd.

11F, Block C North Building, Raycom InfoTech Park, Beijing

mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人: 城市猎人 <423689835@qq.com>

发送时间: 2021 年 4 月 13 日 16:51

收件人: Jia Wei <jiawei@cmgos.com>

主题: 回复: 回复: [案例号: CAS-04004-N2H1M1] % 经销商南宁市纪云科技有限公司反馈客户来宾市住房和城乡建设局蓝屏问题 % 初次响应 CMIT:0001184

意思说还需要蓝屏一次再收集这个日志,

---原始邮件---

发件人: "Jia Wei" <jiawei@cmgos.com>

发送时间: 2021 年 4 月 13 日(周二) 下午 4:49

收件人:

"624687084"<624687084@qq.com>; "423689835@qq.com"<423689835@qq.com>;

抄送: "Case_Notification"<Case_Notification@cmgos.com>;

主题: 回复: [案例号: CAS-04004-N2H1M1] % 经销商南宁市纪云科技有限公司
反馈客户来宾市住房和城乡建设局蓝屏问题 % 初次响应 CMIT:0001184

覃先生, 您好,

刚刚电话未能联系到您, 已经收到您上传的日志文件。但目前还需要 Full Dump 文件进行问题定位。

您可以在 2021 年 4 月 6 日(星期二) 下午 5:57 的邮件中找到配置 dump 的方法。蓝屏之后可以到邮件中指定位置收集日志文件, 压缩后上传。

贾伟 Jia Wei

神州网信技术有限公司

服务支持电话: 400-818-0055

电子邮箱: jiawei@cmgos.com

C&M Information Technologies Co., Ltd.

11F, Block C North Building, Raycom InfoTech Park, Beijing

mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人: Jia Wei

发送时间: 2021 年 4 月 8 日 9:22

收件人: '624687084' <624687084@qq.com>; '423689835@qq.com' <423689835@qq.com>

抄送: Case_Notification <Case_Notification@cmgos.com>

主题: 回复: [案例号: CAS-04004-N2H1M1] % 经销商南宁市纪云科技有限公司
反馈客户来宾市住房和城乡建设局蓝屏问题 % 初次响应 CMIT:0001184

您好!

之前已经与覃先生电话沟通, 基于沟通的结果, 后续覃先生会安排时间进行问题复现和日志收集工作。

收到日志文件后我将立刻着手进行问题分析。

贾伟 Jia Wei
神州网信技术有限公司
服务支持电话: 400-818-0055
电子邮箱: jiawei@cmgos.com

C&M Information Technologies Co., Ltd.
11F, Block C North Building, Raycom InfoTech Park, Beijing
mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人: 624687084 <624687084@qq.com>

发送时间: 2021 年 4 月 7 日 18:30

收件人: Jia Wei <jiawei@cmgos.com>

主题: 回复: 回复: [案例号: CAS-04004-N2H1M1] % 经销商南宁市纪云科技有限公司
反馈客户来宾市住房和城乡建设局蓝屏问题 % 初次响应 CMIT:0001184

贾伟工程师您好, 现在这个案例有什么新的进展了嘛?

----- 原始邮件 -----

发件人: "Jia Wei" <jiawei@cmgos.com>;

发送时间: 2021 年 4 月 6 日(星期二) 下午 5:57

收件

人: "624687084"<624687084@qq.com>;"423689835@qq.com"<423689835@qq.com>;

抄送: "Case_Notification"<Case_Notification@cmgos.com>;

主题: 回复: [案例号: CAS-04004-N2H1M1] % 经销商南宁市纪云科技有限公司
反馈客户来宾市住房和城乡建设局蓝屏问题 % 初次响应 CMIT:0001184

张先生, 您好!

问题定义:

经销商为用户重装系统, 使用一段时间后电脑发生蓝屏问题,

联想客服检查排除硬件问题, 经销商反馈, 用户只安装日常办公软件, 无安装特殊软件和驱动程序

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。

日志收集:

一、按照附件《Full Dump 配置常规方案》对 dump 日志进行设置

设置完毕后, 等待出现蓝屏现象, 在 C:\Windows\MEMORY.DMP 文件压缩并上传。

二、工具收集

1) 首先, 在**有问题的 CMGE 系统上**, 下载附件 zip 文件并解压到本地磁盘。之后双击运行 exe 文件, 同意隐私声明后, 按照下图勾选系统日志, 组策略信息、网络信息、软件信息, 系统进程、已安装补丁, 点击收集。

2) 收集完毕后将当前用户桌面生产 CMGE_Log。点击确定, 将直接打开文件夹并定为压缩文件。

<[A09399C1@EC5E0C75.1DC68060.jpg](#)>

<[CB55072B@2668722A.1DC68060.jpg](#)>

3) 将日志文件上传。

数据上传与下载

Filezilla client 端下载 URL: <https://filezilla-project.org/download.php?type=client>

主机: sftp://ocean.cmgos.com

用户名为: lbszjj

密码: 1234.asd

端口: 22222

登陆后选择 Upload 文件夹上传。

<[F1BB0DFC@C81ED42B.1DC68060.jpg](#)>

贾伟 Jia Wei

神州网信技术有限公司

服务支持电话: 400-818-0055

电子邮箱: jiawei@cmgos.com

C&M Information Technologies Co., Ltd.

11F, Block C North Building, Raycom InfoTech Park, Beijing

mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人: Jia Wei <jiawei@cmgos.com>

发送时间: 2021 年 4 月 6 日 17:23

收件人: 张紫林 <624687084@qq.com>

抄送: Jia Wei <jiawei@cmgos.com>

主题: [案例号: CAS-04004-N2H1M1] % 经销商南宁市纪云科技有限公司反馈客户来宾市住房和城乡建设局蓝屏问题 % 初次响应 CMIT:0001184

张紫林 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 贾伟 。 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-04004-N2H1M1 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”。