

王先生 您好:

感谢您的电话接听, 经过您的同意, 我将暂时归档此案例。

工单的归档并不会影响我们为您提供技术支持服务, 如您有其他问题, 您可以致电技术支持热线 4008180055。

案例总结:

问题定义:

用户电脑开机运行一会儿后, 出现蓝屏问题, 需要协助分析。

问题总结:

近期末再出现蓝屏问题, 可以暂时关闭案例, 后续出现蓝屏问题, 可以联系 CMIT 继续处理。

案例进展:

dump 文件显示错误代码为 0x139, 这表明系统检测到关键数据结构损坏。

系统函数在执行过程中检测发现了_LIST_ENTRY 损坏导致了蓝屏, dump 中未得到更明确的错误信息。

但是出现这种错误的常见原因可能有: 错误的驱动程序、硬件变化或者病毒损坏系统文件等。

建议更新旧版本驱动并安装操作系统最新更新补丁。

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.

服务电话: 4008180055

电子邮箱: weiliang@cmgos.com

官方网站: www.cmgos.com

发件人: Wei Liang

发送时间: 2022 年 4 月 25 日 10:59

收件人: 王先生; 627703743@qq.com

抄送: Case_Notification

主题: 答复: [案例号: CAS-06077-R1R0G6] % 贵州双龙航空港经济区贵龙社区服务中心用户反馈设备蓝屏问题 % 初次响应 CMIT:0001249

王先生 您好:

刚刚给您的电话没有接通。

来信是想咨询当前案例进展状况。您与最终用户沟通确认时间可以远程查看故障机情况后，可以通过邮件或者热线电话 4008180055 联系我们。

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。

危亮 Wei Liang

神州网信技术有限公司

C&M Information Technologies Co.,Ltd.

服务电话: 4008180055

电子邮箱: weiliang@cmgos.com

官方网站: www.cmgos.com

发件人: Wei Liang

发送时间: 2022 年 4 月 20 日 11:32

收件人: 王先生; 627703743@qq.com

抄送: Case_Notification

主题: 回复: [案例号: CAS-06077-R1R0G6] % 贵州双龙航空港经济区贵龙社区服务中心用户反馈设备蓝屏问题 % 初次响应 CMIT:0001249

王先生 您好:

分析您上传的 dmp 文件, 其蓝屏错误代码为 0x139, 这表明系统检测到关键数据结构损坏。进一步查看 dmp 中的 call stack 和 windbg 自动分析信息:

STACK_TEXT:

00 fffff938e`e5cc2d28 ffffff802`141d65e9	nt!KeBugCheckEx
01 fffff938e`e5cc2d30 ffffff802`141d6990	nt!KiBugCheckDispatch+0x69
02 fffff938e`e5cc2e70 ffffff802`141d4d8e	nt!KiFastFailDispatch+0xd0
03 fffff938e`e5cc3050 ffffff802`1420a2ee	nt!KiRaiseSecurityCheckFailure+0x30e
04 fffff938e`e5cc31e0 ffffff802`1407b108	nt!KiSwapThread+0x18efae
05 fffff938e`e5cc32a0 ffffff802`14078e12	nt!KiCommitThreadWait+0x508
06 fffff938e`e5cc3340 ffffff802`146c38da	nt!KeWaitForMultipleObjects+0x582
07 fffff938e`e5cc3410 ffffff802`146c34e1	nt!ObWaitForMultipleObjects+0x2aa
08 fffff938e`e5cc3910 ffffff802`141d6008	nt!NtWaitForMultipleObjects32+0xf1
09 fffff938e`e5cc3b90 00000000`771c1cbc	nt!KiSystemServiceCopyEnd+0x28
0a 00000000`0634ee38 00000000`00000000	0x771c1cbc

SYMBOL_NAME: nt!KiSwapThread+18efae

MODULE_NAME: [nt](#)

IMAGE_NAME: ntkrnlmp.exe

STACK_COMMAND: .thread ; .cxr ; kb

BUCKET_ID_FUNC_OFFSET: 18efae

FAILURE_BUCKET_ID: 0x139_3_CORRUPT_LIST_ENTRY_KTIMER_LIST_CORRUPTION_nt!KiSwapThread










OS_VERSION: 10.0.17763.1

显示由 32 位地址 0x771c1cbc 跳转到了系统调用，系统函数在执行过程中检测发现了 _LIST_ENTRY 损坏导致了蓝屏，dump 中未得到更明确的错误信息。
但是出现这种错误的常见原因可能有：**错误的驱动程序、硬件变化或者病毒损坏系统文件等**。
查看 dump 中显示加载的驱动情况，有几个驱动版本如 hostnt.sys、atikmdag.sys 比较旧，请确认这些驱动版本是否可以更新。

```
start      end      module name
fffff802`13630000 fffff802`13637000  HOSTNT      (deferred)
Image path: \SystemRoot\System32\Drivers\HOSTNT.SYS
Image name: HOSTNT.SYS
Browse all global symbols functions data
Timestamp:   Tue Nov 27 10:16:37 2007 (474B7E05)
Checksum:    0000BC80
ImageSize:   00007000
Translations: 0000.04b0 0000.04e4 0409.04b0 0409.04e4
Information from resource tables:

0: kd> lmDvmatikmdag
Browse full module list
start      end      module name
fffff802`1a9c0000 fffff802`1becf000  atikmdag    (deferred)
Image path: \SystemRoot\system32\DRIVERS\atikmdag.sys
Image name: atikmdag.sys
Browse all global symbols functions data
Timestamp:   Tue Sep 1 09:32:19 2015 (55E50023)
Checksum:    014AB39C
ImageSize:   0150F000
```

查看系统日志，发现出现 bugcheck 记录大概的时间在 2022.1.11 和 2022.4.11 最近几天比较频繁。

级别	日期和时间	来源	事件 ID	任务
 错误	2022/4/15 16:02:38	BugCheck	1001	无
 错误	2022/4/15 15:37:57	BugCheck	1001	无
 错误	2022/4/15 14:17:21	BugCheck	1001	无
 错误	2022/4/14 11:47:19	BugCheck	1001	无
 错误	2022/4/12 14:14:27	BugCheck	1001	无
 错误	2022/4/12 14:09:51	BugCheck	1001	无
 错误	2022/4/11 19:18:04	BugCheck	1001	无
 错误	2022/1/11 10:12:49	BugCheck	1001	无
 错误	2022/1/11 9:55:20	BugCheck	1001	无

事件 1001，BugCheck

常规

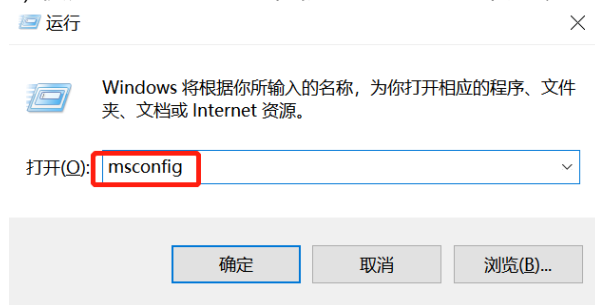
详细信息

计算机已经从检测错误后重新启动。检测错误: 0x00000139 (0x0000000000000003, 0xffff938ee5cc3050, 0xffff938ee5cc2fa)

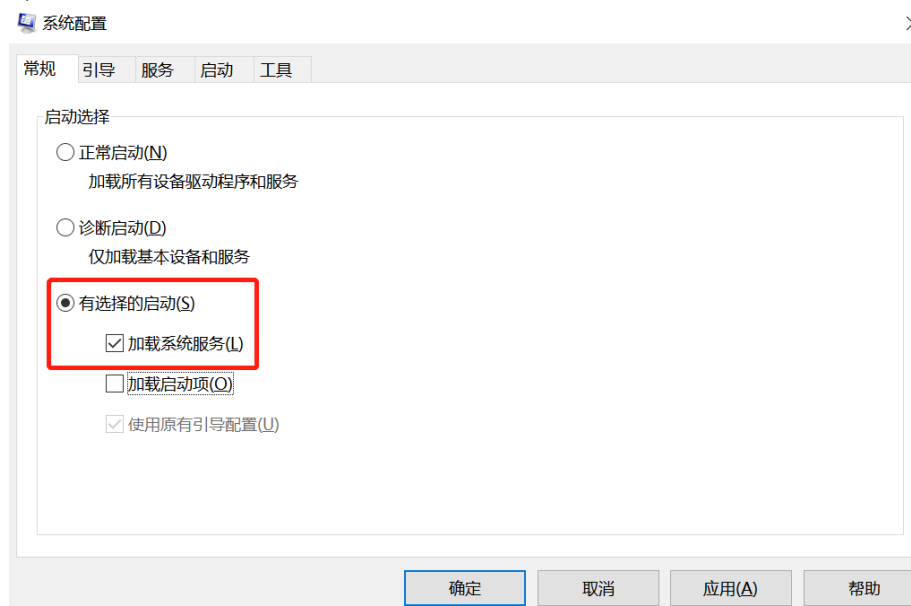
日志显示在 2022.1.11 那段时间 ntfs 文件系统出现问题，这时候出现一些蓝屏问题有可能与 ntfs 文件系统出现问题有关。
2022.4.11 开始这几天出现的蓝屏代码大致为：0x139,0x50,0x1a,0x3b。这些蓝屏代码都是内存相关的错误代码。

基于这些信息，有以下几个问题需要您确认：

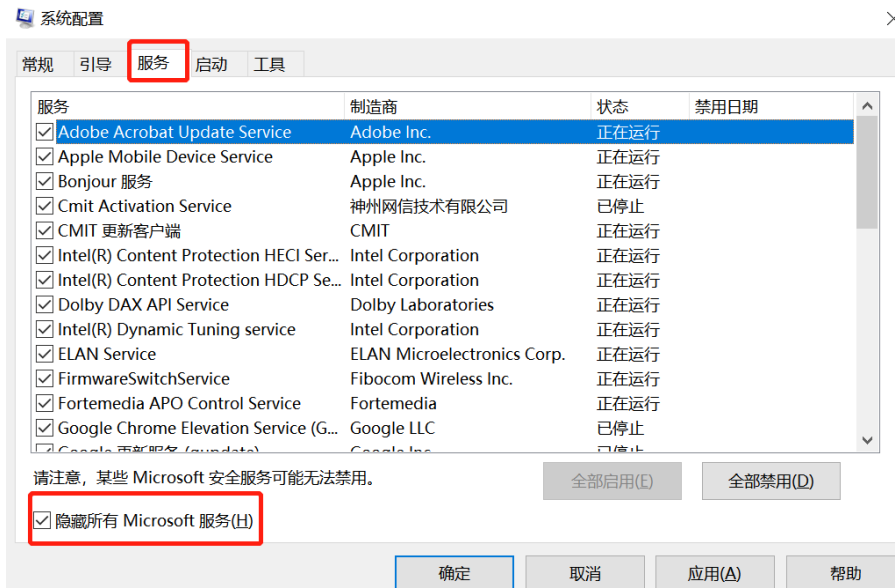
- 1) 2022.4 月这段时间是否有新的硬件变化或者应用安装、驱动变化。
- 2) 查看设备管理器中驱动情况，是否有一些硬件显示黄叹号提示。
- 3) 尝试更新旧版本驱动并安装操作系统最新更新。
- 4) 使用安全软件扫描、检测系统安全状态。
- 5) 尝试配置 clean boot 启动验证。具体操作如下：
 - a) 使用 Windows + R 快捷键打开“运行”窗口，执行 msconfig 命令



- b) 在“系统配置”的“常规”选项卡中选择“有选择的启动”选项，再取消勾选“加载启动项”。



- c) 点击“服务”选项卡，勾选底部的“隐藏所有 Microsoft 服务”，点击“确定”。



d) 重启计算机观察运行情况。

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 4 月 18 日 14:40

收件人: '王先生' <llslbsc@163.com>; '627703743@qq.com' <627703743@qq.com>

抄送: Case_Notification <Case_Notification@cmgos.com>

主题: 回复: [案例号: CAS-06077-R1R0G6] % 贵州双龙航空港经济区贵龙社区服务中心用户反馈设备蓝屏问题 % 初次响应 CMIT:0001249

王先生 您好:

您上传的日志已经收到, 如有任何进展会及时和您联系。

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: 2022 年 4 月 15 日 17:38

收件人: 王先生 <llslbse@163.com>; '627703743@qq.com' <627703743@qq.com>

抄送: Case_Notification <Case_Notification@cmgos.com>

主题: 回复: [案例号: CAS-06077-R1R0G6]% 贵州双龙航空港经济区贵龙社区服务中心用户反馈设备蓝屏问题 % 初次响应 CMIT:0001249

王先生 您好:

刚刚给您的电话没有接通。

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:

用户电脑开机运行一会儿后, 出现蓝屏问题, 需要协助分析。

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。

一、需要您确认设备在开机正常运行未出现蓝屏问题这段时间内,

a) 查看系统分区是否有 dmp 文件 **C:\Windows\MEMORY.DMP**, 请您复制这个文件。

b) 下载附件的 CMGELogCollector.zip, 解压后在故障机上运行 CMGELogCollector.exe, **勾选全部选项**, 点击“收集”, 运行几分钟后会在桌面生成日志压缩包。



请您压缩 MEMORY.DMP 文件和日志压缩包，通过 CDUC 一块上传。

二、如果设备无法正常运行，请您从 PE U 盘启动进入 PE 系统，查看设备的系统分区，复制 Windows\Logs 目录、Windows\System32\winevt 目录和 Windows\MEMORY.DMP 文件。（如果 Windows\minidump 目录存在，也复制 minidump 目录。）将所有的相关文件压缩后通过 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：guizhou

密码：guizhou

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 4 月 15 日 16:46
收件人: 王先生 <llslbcs@163.com>
抄送: Wei Liang <weiliang@cmgos.com>
主题: [案例号: CAS-06077-R1R0G6] % 贵州双龙航空港经济区贵龙社区服务中心用户反馈设备蓝屏问题 % 初次响应 CMIT:0001249

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-06077-R1R0G6 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”。