

李先生，您好：

如之前电话沟通，由于当前问题电脑均已格式化重装，问题无法再次复现供后续分析，经您同意，此 case 将暂做归档处理，以下为案例总结，请您知悉：

Case No: CAS-04863-W5Z5X4

问题描述：

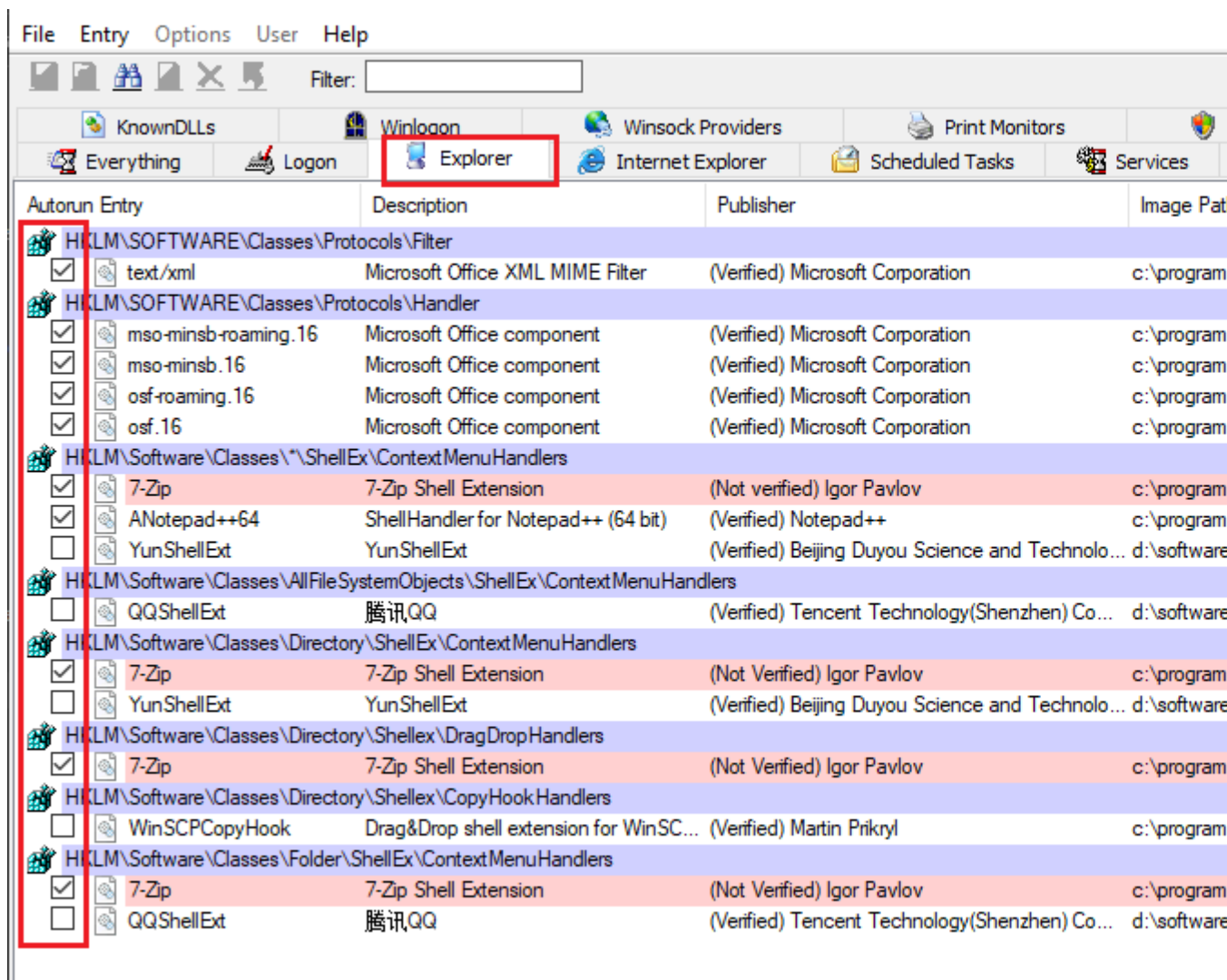
=====

用户反馈 V2020-L 连续出现开机黑屏只显示鼠标的现象。型号为：联想 M820T,联想 920T，戴尔 optiplex 7070，重新打开 explorer.exe 进程无效，安全模式无法进入，还原系统失败，只能格式化重装系统。

问题总结：

=====

1. 从启动日志上，dwm 和 explorer 的进程未看到异常内容，不排除三方线程造成桌面窗口调用 hang 住的情况，如：c:\wincows\syswow64\pclient 和 c:\program files(x86)\Asiainfo security\officeScan client
2. 后续如再发生该类问题，也可使用 Autoruns 工具，将 explorer 下所有的插件取消勾选，重启 explorer 进程看是否问题还存在，工具下载链接：<https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns>



3. 如果没有效果，进一步需要配置 complete dump，重启生效后登陆系统，保持黑屏状态 10 分钟，然后触发 dump。

以上，经您的确认，此 case 将暂做归档处理，您可以在方便时随时与我们联系做进一步问题排查，谢谢。

李琦 Li Qi
 神州网信技术有限公司
 C&M Information Technologies Co.,Ltd.
 服务支持电话： 4008180055
 电子邮箱 Email: liqi@cmgos.com



神州网信
CMIT

发件人: Li Qi

发送时间: 2021 年 10 月 13 日 17:30

收件人: '李金鑫' <459963801@qq.com>

抄送: ICBC_Notification <ICBC_Notification@cmgos.com>; '吴毓杰'

<win10sup@sdicbc.com.cn>

主题: 回复: [案例号: CAS-04863-W5Z5X4] % |P2|ICBC|分行电脑黑屏无法启动 % 初次响应
CMIT:0001532

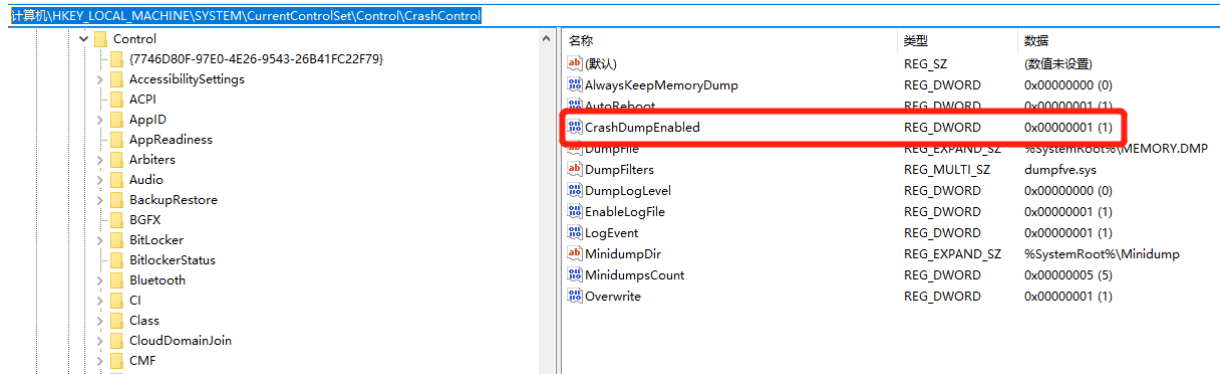
李先生, 您好:

请按如下步骤收集 dump 文件供进一步分析, 谢谢

1, 在运行窗口输入 regedit, 打开注册表编辑器,

导航至: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl

将 CrashDumpEnabled 注册表项设置为 1

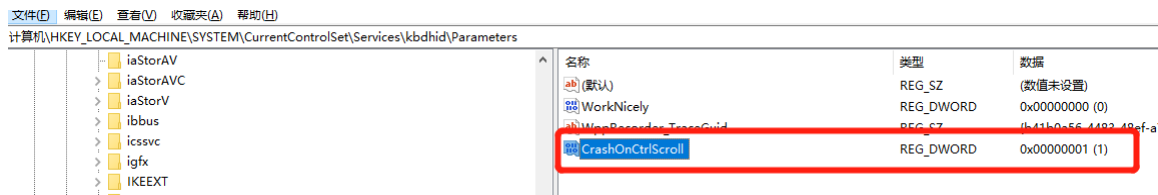


2, 导航至: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kbdhid\Parameters]

创建如下键值: Key name: CrashOnCtrlScroll

Key type: DWORD32

Key value: 00000001



3, 重启电脑使其生效

4, 进入黑屏后, 使用 USB 键盘触发 dump: 右边的 ctrl 键按住不放, 连接两次 scroll lock 键。内存转储触发后, 您能看到类似如下界面:

```
A problem has been detected and windows has been shut down to prevent damage
to your computer.

DRIVER_IRQL_NOT_LESS_OR_EQUAL

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x000000D1 (0xE1C54008, 0xD0000002, 0x00000000, 0xF8983579)

*** myfault.sys - Address F8983579 base at F8983000, DateStamp 4d26670c

Beginning dump of physical memory
Dumping physical memory to disk: 18
```

5, Dumping 至 100%后, 电脑将自动重启。dump 文件会产生在 c:\windows\memory.dmp。请您检查 memory.dmp 是否增长, 当停止增长后, 请收集此文件。

李琦 Li Qi
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话: 4008180055
电子邮箱 Email: liqi@cmgos.com



发件人: Li Qi
发送时间: 2021 年 10 月 12 日 14:36
收件人: 李金鑫 <459963801@qq.com>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>; '吴毓杰'
<win10sup@sdicbc.com.cn>
主题: 回复: [案例号: CAS-04863-W5Z5X4] % |P2|ICBC|分行电脑黑屏无法启动 % 初次响应
CMIT:0001532

李先生, 您好:

如刚才电话沟通，我谨以此邮件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 V2020-L 连续出现开机黑屏只显示鼠标的现象。型号为：联想 M820T,联想 920T，戴尔 optiplex 7070，重新打开 explorer.exe 进程无效，安全模式无法进入，还原系统失败，只能格式化重装系统。

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。

以下是需要您收集的日志内容，工具可保存附件获得：

CMGELogCollector 使用方法：

1) 在复现问题的计算机上保存附件 CMGELogCollector.zip 文件并解压到本地磁盘，双击运行 exe 文件，同意隐私声明后，按照下图勾选，点击收集。



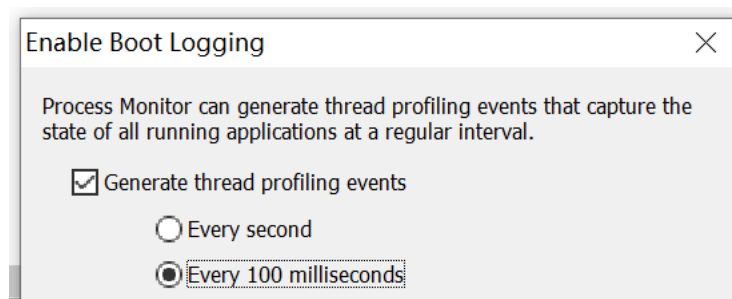
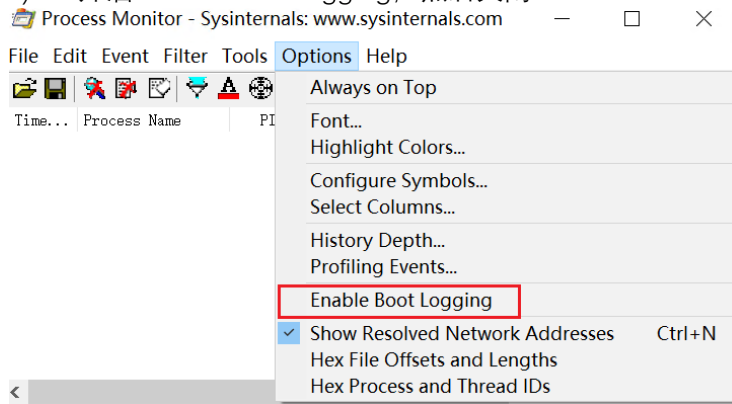
2) 收集完毕后将在当前用户桌面生产 CMGE_Log。点击确定，将直接打开文件夹并定为压缩文件。



3) 将压缩文件上传至 CDUC 上传系统。

ProcessMonitor 使用方法:

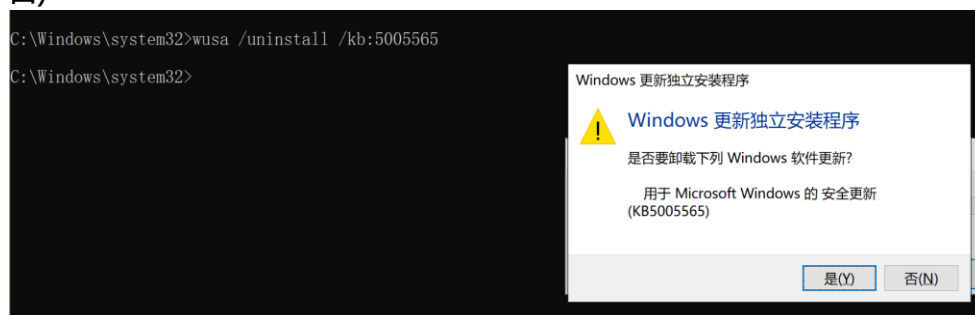
- a) 保存附件 ProcessMonitor.zip 至故障计算机
- b) 解压完成后, 双击执行 procmon.exe
- c) 开启 Enable Boot Logging, 然后关闭 Process Monitor



- d) 重启电脑, 待进入系统黑屏后, 查看 C:\Windows\procmon.pmb, 并将此文件回传给我进行分析, 谢谢

卸载补丁更新方法:

打开 C:\Windows\System32 目录, 找到 cmd.exe, 单击选中后右键, 菜单中选择“以管理员身份运行”, 输入 `wusa /uninstall /kb: 5005030`(KB5005030 为 2021.8 月累积更新, 下图仅为示例图)



日志上传:

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

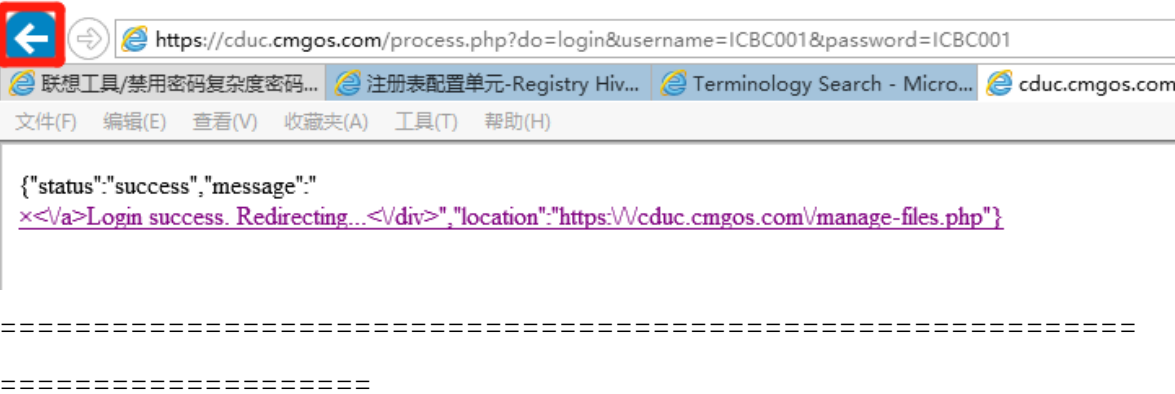
用户名：ICBC001

密码：ICBC001

添加文件后点击上传文件 ,上传完毕后点击保存



注意，如果遇到如下所示页面，点击后退即可看到页面



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。

李琦 Li Qi
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话： 4008180055
电子邮箱 Email: liqi@cmgos.com



发件人: Li Qi <liqi@cmgos.com>
发送时间: 2021 年 10 月 12 日 11:10
收件人: 李金鑫 <459963801@qq.com>

抄送: Li Qi <liqi@cmgos.com>

主题: [案例号: CAS-04863-W5Z5X4] % |P2|ICBC|分行电脑黑屏无法启动 % 初次响应
CMIT:0001532

李金鑫 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 李琦。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-04863-W5Z5X4 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”。