

叶先生 & 毓杰，您好：

如刚才电话沟通，目前客户已知悉 CPU 冲高的原因，并着手三方软件厂商进行处理，经用户同意，此 case 将暂做归档处理，以下为案例总结，请您知悉：

Case No: CAS-05064-Z3P1T6

**问题描述：**

=====

用户反馈连续两天出现笔记本电脑 CPU 冲高现象，导致电脑卡顿严重。

**问题总结：**

=====

用户反馈在插拔网线时出现 CPU 冲高的问题，该问题经查看 xperf 日志，发现占用高 CPU 的系统进程为 ntosknel，主要工作为开启相关线程，并等待 tmxpflt.sys 的返回句柄及上下文切换，属正常系统行为，而开启线程的发起由亚信防病毒软件，应由亚信厂商进行进一步协查，据用户反馈，亚信已调整部分服务器配置，并且由于相关动作与 TMS 相关，应进一步由双方判断其逻辑的合理性进行调整，目前判断与操作系统无关，同意暂时归档此案例。

以上，经用户确认，此 case 将暂做归档处理，如您有其他问题可随时与我们联系，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](mailto:liqi@cmgos.com)



**神州网信**  
CMIT

发件人: Li Qi  
发送时间: 2021 年 11 月 19 日 15:53  
收件人: '叶家杰' <yejj@sdc.icbc.com.cn>; '吴毓杰' <win10sup@sdc.icbc.com.cn>  
抄送: ICBC\_Notification <ICBC\_Notification@cmgos.com>  
主题: 回复: [案例号: CAS-05064-Z3P1T6 ] % |P2|ICBC|工行笔记本 CPU 冲高问题 % 初次响应 CMIT:0001948

叶先生 & 毓杰, 您好:

如刚才电话沟通, 以下为您收集的 xperf 日志的分析结果, 供您参考:

日志背景:

插入网线, CPU 使用率升高, 运行 xperf 8 分钟, 记录 CPU 的使用率情况。

日志结果:

Lin...	Thread Activity Tag	Process	Thread ID	Switch-In Time (s)	CPU	CPU Usage (in... Sum
1						2,086,369.082492
2		System (4)				463,856.080543
3		services.exe (816)				347,865.984285
4		idea64.exe (11208)				237,992.102884
5		scclient.exe (15172)				143,158.351701
6		dlmshr.exe (12356)				101,842.140731

从日志来看, system 进程占用 CPU 最高。(Gscfmg.sys 的权重也相对较高, 但考虑到用户发生问题的触发动作为插入网线, 需要进行网络认证的执行操作, 因此认为在正常值范围。)

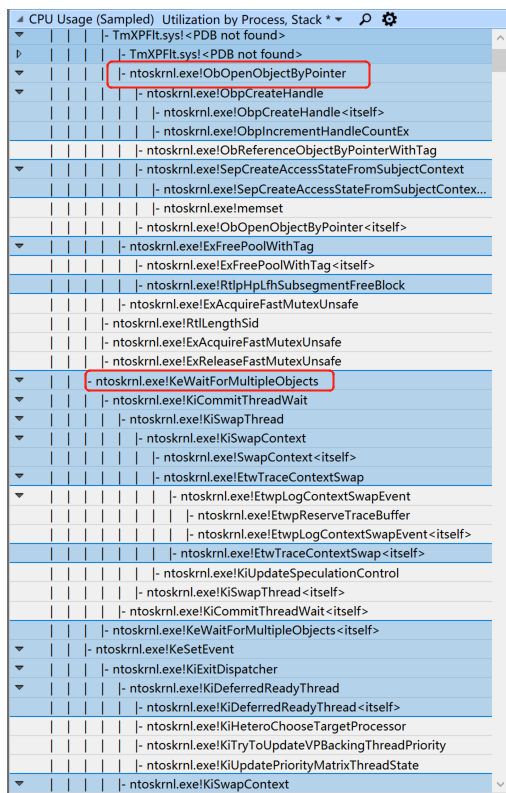
进一步查看该进程的使用权重, 可以看到其中 ntoskrnl.exe 占比最大, 做的最主要的工作就是 start thread。

Lin...	Process	Stack	Count	Sum	Weight (in view) (ms)	Sum
1	System (4)		461,388		461,399.324697	
2		[Root]	461,326		461,337.316997	
3		ntoskrnl.exe!KiStartSyste...	257,912		257,903.122024	
4		gscfmg.sys!<PDB not fou...	149,467		149,480.801333	
5		VSApiNt.sys!<PDB not fou...	46,435		46,441.005935	
6		netmgr.sys!<PDB not fou...	4,507		4,507.377997	
7		krnlmgr.sys!<PDB not fou...	2,247		2,246.897908	
8		krnlmgr.sys!<PDB not fou...	262		262.050006	

继续展开来看, 可以看到 ntoskrnl.exe 的大部分工作与 tmxpfilt.sys 的执行程序有关。

3		ntoskrnl.exe!PspSystemT...	257,912		257,903.122024	
4		ntoskrnl.exe!PspSystemT...	257,912		257,903.122024	
5		TmxPflt.sys!<PDB not...	248,893		248,884.772857	
6		TmxPflt.sys!<PDB not...	248,893		248,884.772857	
7		TmxPflt.sys!<PDB n...	248,812		248,803.727258	
8		TmxPflt.sys!<PD...	248,808		248,799.734058	

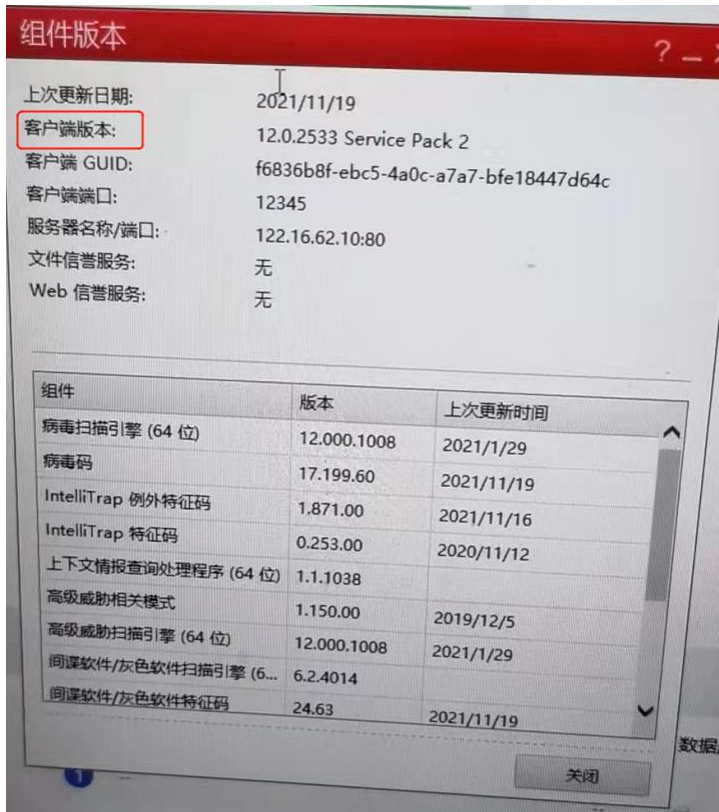
而 ntoskrnl 之所以占用较高的 CPU 使用, 是在等待 tmxpfilt.sys 的返回句柄及上下文切换等动作。



@'吴毓杰', 经查询, TmXPFlt.sys 属于亚信防病毒软件的组件, 由于没有其对应的 symbol 文件, 所以无法解析在日志收集过程中其具体的执行逻辑, 建议联系亚信进行进一步排查。

▼					TmXPFlt.sys!<PDB not...	248,893	248,884.772857
					TmXPFlt.sys!<PDB not...	248,893	248,884.772857
▼					TmXPFlt.sys!<PDB n...	248,812	248,803.727258
▼					TmXPFlt.sys!<PD...	248,808	248,799.734058
▶					TmXPFlt.sys!<...	248,783	248,774.733259

另外叶先生, 请确认问题电脑的亚信防病毒软件是否与以下截图一致, 如不一致, 请及时反馈:



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](mailto:liqi@cmgos.com)



发件人: Li Qi  
发送时间: 2021 年 11 月 16 日 15:01  
收件人: '叶家杰' <[yejj@sdc.icbc.com.cn](mailto:yejj@sdc.icbc.com.cn)>; '吴毓杰' <[win10sup@sdc.icbc.com.cn](mailto:win10sup@sdc.icbc.com.cn)>  
抄送: ICBC\_Notification <[ICBC\\_Notification@cmgos.com](mailto:ICBC_Notification@cmgos.com)>  
主题: 回复: [案例号: CAS-05064-Z3P1T6 ] % |P2|ICBC|工行笔记本 CPU 冲高问题 % 初次响应 CMIT:0001948

叶先生, 您好:

如昨天电话沟通，请确认是否移除 c:\windows\temp 下的 cpuz 的 sys 文件，CPU 性能可以得到缓解。另外，为方便您对日志进行收集，有关于第二个和第三个日志，您可以双击附件及下载链接的脚本进行操作。

第二个 perfmon 日志：下载并解压附件脚本，以管理员身份运行即可。

第三个 xperf 日志：已更新下方下载链接文件，请重新下载并解压，执行 run-xperf.bat 的脚本文件即可。

<https://cdm.cmgos.com/download.php?id=328&token=BLVzglQEYKaOQB0xuFOOyK8xbXjQan>

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](mailto:liqi@cmgos.com)



---

**发件人:** Li Qi  
**发送时间:** 2021 年 11 月 11 日 17:07  
**收件人:** '叶家杰' <[yeji@sdc.icbc.com.cn](mailto:yeji@sdc.icbc.com.cn)>; '吴毓杰' <[win10sup@sdc.icbc.com.cn](mailto:win10sup@sdc.icbc.com.cn)>  
**抄送:** ICBC\_Notification <[ICBC\\_Notification@cmgos.com](mailto:ICBC_Notification@cmgos.com)>  
**主题:** 回复: [案例号: CAS-05064-Z3P1T6 ] % |P2|ICBC|工行笔记本 CPU 冲高问题 % 初次响应 CMIT:0001948

叶先生，您好：

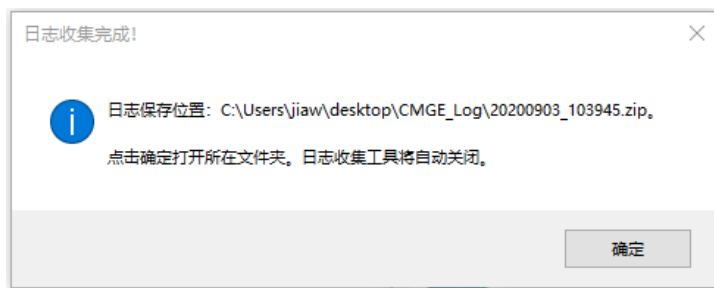
如刚才电话沟通，请帮忙在问题电脑上收集如下几个日志，最好可以提供发生资源消耗过高问题时的时间：

CMGE 系统日志：

1) 请下载附件 CMGELogCollector.zip，解压并运行 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。

#### Perfmon 日志:

1) 请使用管理员帐户运行命令行窗口，并设置以间隔 1 分钟，使用 500MB 循环日志文件的方式收集性能监视日志:

```
Logman.exe create counter Perf-1Minute -f bincirc -max 500 -c "\\LogicalDisk(*)\\*"
"\\Memory\\*" "\\Network Interface(*)\\*" "\\Paging File(*)\\*"
"\\PhysicalDisk(*)\\*" "\\Server\\*" "\\System\\*" "\\Process(*)\\*"
"\\Processor(*)\\*" "\\Cache\\*" -si 00:01:00 -o C:\PerfMonLogs\Perf-1Minute.blg
```

2) 插入网线，当问题电脑出现资源消耗过高问题时，使用以下命令开启（如实在无法开启，可以先运行此命令，然后再插入网线，等待问题复现）:

```
Logman start Perf-1Minute
```

3) 当问题持续 5-10 分钟后，拔下网线，并使用以下命令结束:

```
Logman stop Perf-1Minute
```

4) 将 C:\PerfMonLogs\Perf-1Minute.blg 压缩并上传至 CDUC 上传系统。

XPERF 日志:

1) 从以下链接下载 XPERF 工具:

<https://cduc.cmgos.com/download.php?id=327&token=AfZOmJLWwJQrt5yLqA7z6oIEQGMqCnPt>

2) 使用管理员权限的 cmd 并定位解压后的路径 [Filelocation] \latest, 该路径下输入命令

Xperf.exe -on latency -stackwalk profile

```
D:\>cd Switch
D:\Switch>cd Xperf
D:\Switch\Xperf>cd latest
D:\Switch\Xperf\latest>xperf.exe -on latency -stackwalk profile
D:\Switch\Xperf\latest>_
```

3) 等待 5-10 分钟之后输入 xperf.exe -stop -d merged.etl 并将该目录下生成的 merged.etl

```
D:\Switch\Xperf\latest>xperf.exe -on latency -stackwalk profile
D:\Switch\Xperf\latest>xperf.exe -stop -d merged.etl
Merged Etl: merged.etl
D:\Switch\Xperf\latest>_
```

5) 4) 将该文件压缩并上传至 CDUC 上传系统。

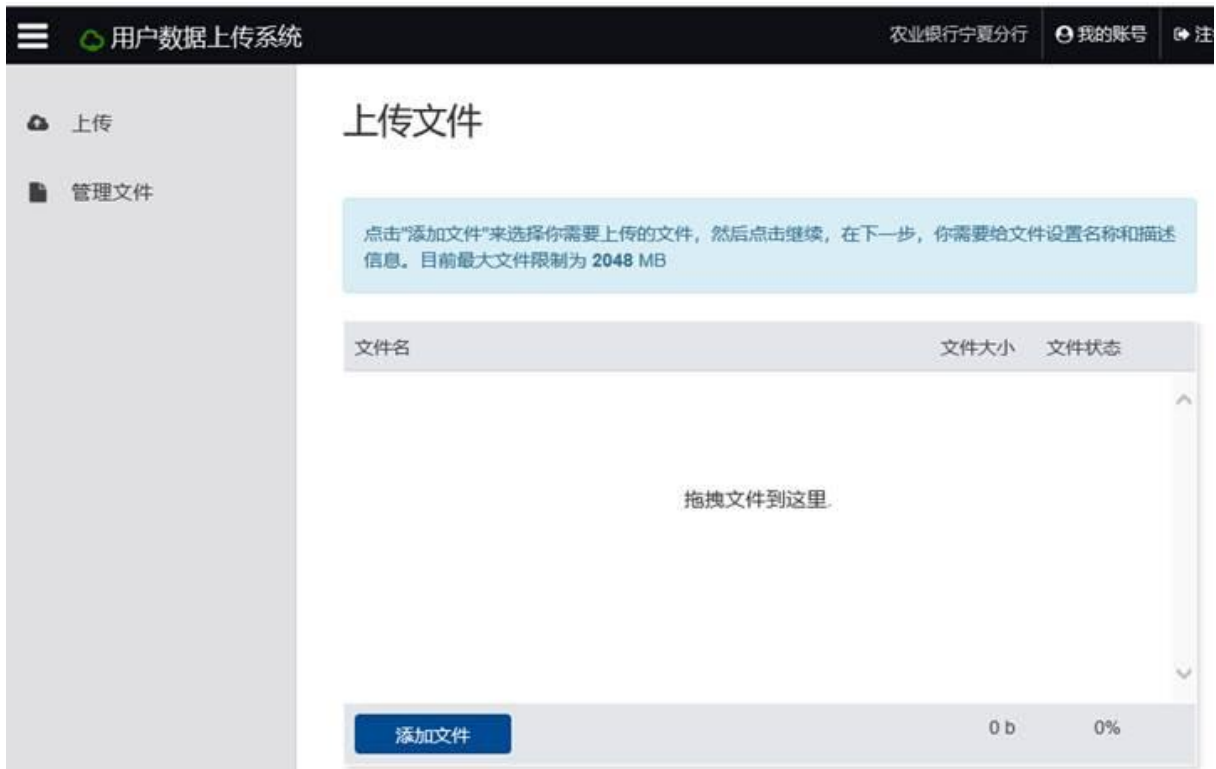
上传日志方法: (@'吴毓杰', 如用户无法上传上述日志, 烦请帮忙上传, 谢谢)

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

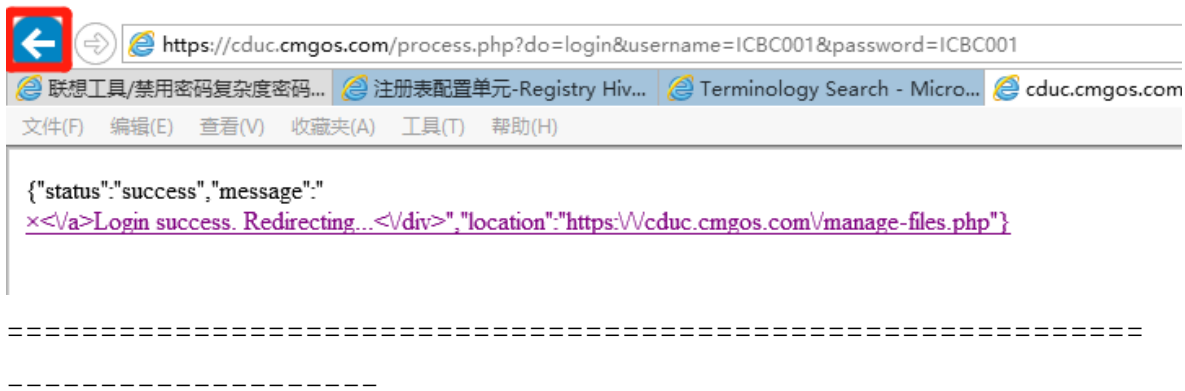
用户名: ICBC001

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](mailto:liqi@cmgos.com)



---

发件人: Li Qi  
发送时间: 2021 年 11 月 11 日 9:58  
收件人: 叶家杰 <[yejj@sdicbc.com.cn](mailto:yejj@sdicbc.com.cn)>  
抄送: ICBC\_Notification <[ICBC\\_Notification@cmgos.com](mailto:ICBC_Notification@cmgos.com)>; '吴毓杰' <[win10sup@sdicbc.com.cn](mailto:win10sup@sdicbc.com.cn)>

**主题:** 回复: [案例号: CAS-05064-Z3P1T6 ] % |P2|ICBC|工行笔记本 CPU 冲高问题 % 初次响应 CMIT:0001948

叶家杰, 您好:

由于电话未联系到您, 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:**

用户反馈连续两天出现笔记本电脑 CPU 冲高现象, 导致电脑卡顿严重。

**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。

鉴于您当前无法确定具体方便处理问题的时间, 我将每两个工作日与您联系一次, 确认该案例的进度, 当然, 如您方便处理该问题, 可随时回复此邮件或拨打 400-818-0055, 我会与您联系处理该问题, 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](mailto:liqi@cmgos.com)



---

**发件人:** Li Qi <[liqi@cmgos.com](mailto:liqi@cmgos.com)>  
**发送时间:** 2021 年 11 月 11 日 9:45  
**收件人:** 叶家杰 <[yejj@sdicbc.com.cn](mailto:yejj@sdicbc.com.cn)>  
**抄送:** Li Qi <[liqi@cmgos.com](mailto:liqi@cmgos.com)>

**主题:** [案例号: CAS-05064-Z3P1T6 ] % |P2|ICBC|工行笔记本 CPU 冲高问题 % 初次响应 CMIT:0001948

叶家杰 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-05064-Z3P1T6 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”。