

许先生 您好:

感谢您的电话接听。

经过您的同意, 我将暂时归档这个案例。

工单的归档并不会影响我们为您提供技术支持服务, 如有其他问题, 您可以随时联系我们。

案例总结:

问题定义:

工行用户反馈有一台设备 V2022-L 版本系统出现了自动重启的问题, 每隔 1 小时重启一次, 需要协助排查。

问题总结:

与工行联系人确认, 同意暂时归档案例。

可以在问题设备上尝试使用 procmon 工具抓取是哪一个应用调用的 shutdown.exe 应用, 具体操作如下:

- 1、先重启问题设备, 记录当前**系统重启的时间**。
- 2、在系统重启后大概 55 分钟左右, 运行 procmon 工具开始抓取日志。
- 3、抓取日志大概 10 分钟左右, 停止 procmon 日志的抓取, 将保存的 pml 日志压缩后, 通过 CDUC 上传。

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 11 月 13 日 15:34

收件人: ICBC 案例通知 <win10sup@sdicbc.com.cn>

抄送: ICBC_Notification <ICBC_Notification@cmgos.com>

主题: 回复: [案例号: CAS-12432-V5P8M4] % |P2|ICBC|工行用户反馈 V2022-L 版本系统自动重启问题 % 初次响应 CMIT:0001956

许先生 您好:

感谢您的电话接听。

如电话中所说, 您当前较忙, 暂无法按照邮件要求收集所需的日志。我计划下周再与您确认问题设备的日志收集情况。

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 11 月 5 日 16:39

收件人: ICBC 案例通知 <win10sup@sdicbc.com.cn>

抄送: ICBC_Notification <ICBC_Notification@cmgos.com>

主题: 回复: [案例号: CAS-12432-V5P8M4] % |P2|ICBC|工行用户反馈 V2022-L 版本系统自动重启问题 % 初次响应 CMIT:0001956

许先生 您好:

查看问题设备的日志, 从系统日志中可以看到基本上是每间隔 1 小时触发了进程

C:\Windows\SysWOW64\shutdown.exe 执行重启操作。

级别	日期和时间	来源	事件 ID	任务类别
信息	2024/11/4 15:42:20	User32	1074	无
信息	2024/11/4 14:40:08	User32	1074	无
信息	2024/11/4 13:38:06	User32	1074	无
信息	2024/11/4 12:36:08	User32	1074	无
信息	2024/11/4 11:33:50	User32	1074	无
信息	2024/11/4 10:30:40	User32	1074	无
信息	2024/11/4 9:24:59	User32	1074	无
警告	2024/11/1 17:38:07	User32	1073	无
信息	2024/11/1 17:38:04	User32	1074	无

事件 1074, User32				
常规 详细信息				
进程 C:\Windows\SysWOW64\shutdown.exe (KFZXDLEST003) 由于以下原因已代表用户 NT AUTHORITY\SYSTEM 启动计算机				
KFZXDLEST003 的重启: 没有找到这个原因的标题				
原因代码: 0x800000ff				

根据计划任务中有配置 shutdown 任务，查看对应的计划任务，与系统日志中的记录并不是一一对应的，而且有执行返回代码 2147943515。

信息	2024/11/4 10:30:30	TaskScheduler	201	操作已完成
信息	2024/11/4 10:30:42	TaskScheduler	201	操作已完成
信息	2024/11/4 10:25:22	TaskScheduler	201	操作已完成

事件 201, TaskScheduler				
常规 详细信息				
任务计划程序已成功完成任务“\1111”、实例“(796385f4-19bd-49e1-982c-a9c112354afc)”、操作“shutdown.exe”，返回代码为				
2147943515。				

返回代码 2147943515 表示“ERROR_SHUTDOWN_IN_PROGRESS”，即系统正在关闭，并未是计划任务正常运行的状态。

经过测试，计划任务运行的 shutdown.exe 路径为 C:\Windows\System32 目录。

而问题设备系统日志记录的进程 shutdown.exe 的路径包含 sysWOW64 目录，判断运行的进程 shutdown.exe 是 32 位应用。

这通常是其他的 32 位应用调用了 shutdown.exe 应用，才会出现这种情况。

您当前已经重命名了 C:\Windows\SysWOW64 目录中的 shutdown.exe 应用的名称，在这种情况下，可以尝试使用 procmon 工具抓取是哪一个应用调用的 shutdown.exe 应用，具体操作如下：

- 1、先重启问题设备，记录当前系统重启的时间。
- 2、在系统重启后大概 55 分钟左右，运行 procmon 工具开始抓取日志。

3、抓取日志大概 10 分钟左右，停止 procmon 日志的抓取，将保存的 pml 日志压缩后，通过 CDUC 上传。

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 11 月 4 日 17:25
收件人: ICBC 案例通知 <win10sup@sdicbc.com.cn>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: [案例号: CAS-12432-V5P8M4] % |P2|ICBC|工行用户反馈 V2022-L 版本系统自动重启问题 % 初次响应 CMIT:0001956

许先生 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：

工行用户反馈有一台设备 V2022-L 版本系统出现了自动重启的问题，每隔 1 小时重启一次，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。

请您使用 CMGE 日志工具收集问题设备的日志，并通过 CDUC 上传给我们排查。有任何进展会及时与您联系沟通，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: Wei Liang <weiliang@cmgos.com>
发送时间: 2024 年 11 月 4 日 16:50
收件人: ICBC 案例通知 <win10sup@sdicbc.com.cn>
抄送: Wei Liang <weiliang@cmgos.com>
主题: [案例号: CAS-12432-V5P8M4] % |P2|ICBC|工行用户反馈 V2022-L 版本系统自动重启问题 % 初次响应 CMIT:0001956

许翔 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-12432-V5P8M4 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”。