许先生 您好:

感谢您的电话接听。

经过您的确认, 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 win7 系统安装补丁 KB4474419 失败,在安装完成重启系统时进度显示 9%左右时重启回滚,但是卸载 TMS 后可以正常安装补丁,需要 CMIT 协助排查导致补丁安装失败的根本原因。

问题总结:

最终用户近期未反馈这个补丁安装问题,同意暂时归档案例。

案例进展:

1、查看 cbs 日志,是由于更新驱动 cpu.inf 失败,导致的系统回滚,补丁 KB4474419 安装失败。

查看 cpu.inf 驱动安装日志,可以看到是在安装 AMD K8 Processor 驱动过程中,在添加 AmdK8 服务时,设置对应的 Start Type 出现 0x00000005(拒绝访问)错误,最终导致整个 cpu.inf 驱动更新失败。

2、安装完 TMS 管控应用后, 注册表路径

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\下部分注册表键值无法修改,如 amdk8、amdppm 项和 devmgr、gscfmgr 等和 TMS 相关的项中的注册表键值,在修改时会提示更新失败,使用 reg 命令行修改时会提示"拒绝访问"错误。在安装应用更新补丁时,涉及到相关的驱动更新出现了 0x00000005(拒绝访问)错误,导致更新补丁安装失败。

- 3、测试中发现,通过在 WinPE 中**删除 C:\windows\system32\drivers\krnImgr.sys** 驱动,使操作系统启动后不再加载 **krnImgr.sys** 驱动后,可以正常修改对应的
 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\amdk8 等的注册表键值。
- 4、krnlmgr.sys 驱动是 TMS 应用的关键驱动,针对当前的案例问题,需要请应用厂商调整其安全策略,允许 C:\Windows\servicing\TrustedInstaller.exe 应用修改、更新相关注册表项中的内容。

在使用过程中,需要 TMS 应用根据不同的使用场景配置合适的安全策略。

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 9 月 19 日 16:17

收件人: ICBC 案例通知 < win10sup@sdc.icbc.com.cn > 抄送: ICBC_Notification < ICBC_Notification@cmgos.com >

主题: 回复: [案例号: CAS-12143-POY2F1] % |P2||CBC|工行用户反馈 Win7 系统补丁安装失

败问题 % 初次响应 CMIT:0001339

许先生 您好:

感谢您的电话接听。

如电话中所说,等您这边忙完近期的事情后,再和您沟通这个案例。

如果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9月12日14:55

收件人: ICBC 案例通知 < <u>win10sup@sdc.icbc.com.cn</u>> **抄送:** ICBC_Notification < ICBC_Notification@cmgos.com>

主题: 回复: [案例号: CAS-12143-P0Y2F1] % |P2||CBC|工行用户反馈 Win7 系统补丁安装失

败问题 % 初次响应 CMIT:0001339

许先生 您好:

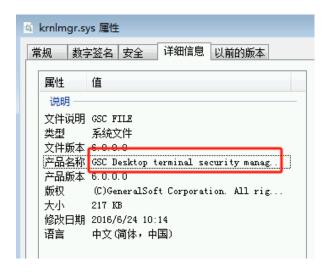
经过一系列的测试、安装完 TMS 管控应用后、注册表路径

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\下部分注册表键值无法修改,如 amdk8、amdppm 项和 devmgr、gscfmgr 等和 TMS 相关的项中的注册表键值,在修改时会提示更新失败,使用 reg 命令行修改时会提示"拒绝访问"错误。在安装应用更新补丁时,涉及到相关的驱动更新出现了 0x000000005(拒绝访问)错误,导致更新补丁安装失败。



测试中发现,通过在 WinPE 中**删除 C:\windows\system32\drivers\krnImgr.sys** 驱动,使操作系统启动后不再加载 **krnImgr.sys** 驱动后,可以正常修改对应的

HKEY LOCAL MACHINE\SYSTEM\CurrentControlSet\Services\amdk8 等的注册表键值。



krnlmgr.sys 驱动是 TMS 应用的关键驱动,针对当前的案例问题,需要请应用厂商调整其安全策略,允许 C:\Windows\servicing\TrustedInstaller.exe 应用修改、更新以下注册表项中的内容。

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AmdK8

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AmdPPM

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\intelppm

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Processor

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ViaC7

并允许将驱动 amdk8.sys、amdppm.sys、intelppm.sys、processor.sys、viac7.sys 复制到C:\Windows\system32\drivers\目录。

在使用过程中,需要 TMS 应用根据不同的使用场景配置合适的安全策略。

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 9 月 10 日 17:14

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

抄送: ICBC_Notification < !CBC_Notification@cmgos.com

主题: 回复: [案例号: CAS-12143-P0Y2F1] % | P2 | ICBC | 工行用户反馈 Win7 系统补丁安装失

败问题 % 初次响应 CMIT:0001339

许先生 您好:

感谢您的电话接听。

查看您提供的问题设备的日志,可以看到安装 KB4474419 失败,报错为: 0x80070005

级别	日期和时间	来源		事件 ID	任务类别
信息	2024/9/10 10:44:48	Servicing		3	无
间信息	2024/9/10 10:23:08	WUSA		2	无
🛕 警告	2024/9/10 10:23:07	WUSA		4	无
间信息	2024/9/10 10:22:51	Servicing		4	无
间信息	2024/9/10 10:21:19	Servicing		1	无
间信息	2024/9/30 17:46:04	Servicing		2	无
事件 3, Servicing					
常规	羊细信息				
Package KB4474419 failed to be changed to the Installed state. Status 0x80070005.					

查看详细的 cbs 日志,是由于更新驱动 cpu.inf 失败,导致的系统回滚,补丁 KB4474419 安装失败。

```
2024-09-10 10:44:35, Info
                                          CBS Doge: [Forward] Installing driver updates, Count
2024-09-10 10:44:36. Info
                                                         INSTALL index: 0, phase: 1, result 0, inf: cpu.inf
                                                 Progress: UI message updated. Operation type: Update. Stage: 1 out of 1. Percent progress
                                          CBS
2024-09-10 10:44:36, Info
                                                         INSTALL index: 0, phase: 2, result 5, inf: cpu.inf
2024-09-10 10:44:44, Info
                                          CBS
2024-09-10 10:44:45, Info
                                          CBS
                                                 Progress: UI message updated. Operation type: Update. Stage: 1 out of 1. Percent progress
2024-09-10 10:44:45, Info
                                          CBS
                                                 DriverUnd
                                      CBS Doge Failed installing driver updates [HRESULT = 0x80070005 - E_ACCESSDENIED]
2024-09-10 10:44:45. Error
                                          CBS
2024-09-10 10:44:45, Info
                                                 Perf.
                                                        Doue. Install end
2024-09-10 10:44:45. Info
                                          CBS
                                                 Failed installing driver updates [HRESULT = 0x80070005 - E ACCESSDENIED]
                                                                                                driver operations queue. [HRESULT = 0x80070
2024-09-10 10:44:45, Error
                                          CBS
                                                 Startup: Rolling back KTM, because drivers failed.
2024-09-10 10:44:45, Info
                                          CBS
                                                  Setting ExecuteState key to: CbsExecuteStateStageDrivers | CbsExecuteStateFlagRollback |
2024-09-10 10:44:46, Info
                                          CBS
2024-09-10 10:44:46. Info
                                          CBS
                                                 Progress: UI message updated. Operation type: Update. Stage: 1 out of 1. Rollback.
2024-09-10 10:44:46, Info
                                                 Progress: UI message updated. Operation type: Update. Stage: 1 out of 1. Rollback.
                                          CBS
                                                 Doge: q-unstage: Inf: cpu.inf, Ranking: 2, Device-Install: 0, Key: 1, Identity: cpu.inf
2024-09-10 10:44:46. Info
                                          CBS
Version=6.1.7601.24384, PublicKeyToken=3lbf3856ad364e35, ProcessorArchitecture=x86, versionScope=NonSxS
2024-09-10 10:44:46, Info
                                          CBS Perf: Doge: Unstaging started.
2024-09-10 10:44:46, Info
                                          CBS
                                                  Doge: [Rollback] Unstaging driver updates, Count 1
                                               Startup: Changing logon timeout to a static timeout: 10800000
2024-09-10 10:44:46, Info
                                          CBS
                                          CBS
                                                         UNSTAGE index: 0, phase: 1, result 0, inf: cpu.inf
2024-09-10 10:44:46, Info
                                          CBS Perf: Doqe: Unstaging ended.
2024-09-10 10:44:46, Info
2024-09-10 10:44:46, Info
                                          CBS Setting ExecuteState key to: CbsExecuteStateFailed
2024-09-10 10:44:46, Info
                                          CBS
                                                 Removed poqexec from Cbs key.
2024-09-10 10:44:46, Info
                                         CBS Removed CCP impactful-commit disabling value.
                                          CBS
2024-09-10 10:44:46, Info
                                                 Doge: Enabling Device installs
                                          CSI 00000006 Cancelling transactions: [1:[77]"TI4.31134493_4116500938:4/Package_for_KB4474419
2024-09-10 10:44:46. Info
2024-09-10 10:44:46, Info
                                         CSI 00000007 Creating NT transaction (seq 1), objectname [6]"(null)"
                                         CSI 00000008 Created NT transaction (seq 1) result 0x00000000, handle @0x210 CSI 00000009@2024/9/10:02:44:47.829 CSI perf trace:
2024-09-10 10:44:46, Info
2024-09-10 10:44:47, Info
CSIPERF:TXCOMMIT:1032406
                                                 Doge Marked package Package_63_for_KB4474419~31bf3856ad364e35~x86~~6.1.3.2 as failed.
                                         CBS
2024-09-10 10:44:47, Error
```

查看 cpu.inf 驱动安装日志,可以看到是在安装 AMD K8 Processor 驱动过程中,在添加 AmdK8 服务时,设置对应的 Start Type 出现 0x00000005(拒绝访问)错误,最终导致整个 cpu.inf 驱动更新失败。

```
{Reflect Driver: AMD K8 Processor}
    sto:
                  Manufacturer = Advanced Micro Devices
                   Section Name = AmdK8 Inst.NT
                  Existing driver file 'C:\Windows\system32\drivers\amdk8.sys' belongs to 'cpu.inf_x86_neutral_729b871528391
    sto:
                 Hardware Id = ACPI\AuthenticAMD_-_x86_Family_15_Model_4
    sto:
                  {Reflect Critical Device: ACPI\AuthenticAMD_-_x86_Family_15_Model_4}
                        Updating critical device 'ACPI#AuthenticAMD_-_x86_Family_15_Model_4'.
    sto:
                        Class GUID = {50127DC3-0F36-415E-A6CC-4CB3BE910B65}
                        Service Name = AmdK8
                   {Reflect Critical Device: exit(0x00000000)}
    sto:
                   {Add Service: AmdK8}
    sto:
                       Updating existing service 'AmdK8'.
!!! sto:
                        Failed to set Start Type. Error = 0x000000005
    sto:
                  {Add Service: exit(0x00000005)}
    sto:
              {Reflect Driver: exit(0x00000005)}
            Failed to reflect driver package. Time = 6926 ms, Error = 0x00000005
!!! sto:
   sto: {Reflect Driver Package: exit(0x00000005)}
!!! sto: Failed to reflect all driver updates. Error = 0x00000005
    Section end 2024/09/10 10:44:45.9/3
<<< [Exit status: FAILURE(0x00000005)]</pre>
```

对比安装补丁成功的设备上的驱动更新过程,可以看到在安装 AMD K8 Processor 驱动过程时,有添加 AmdK8 服务,并复制 amdk8.sys 驱动。

```
sto:
               JAdd Service: AmdK8
                    Updating existing service 'AmdK8'.
sto:
                                    = 0x3 (SERVICE_DEMAND_START)
sto:
                    Start Type
sto:
                    Service Type
                                     = 0x1 (SERVICE KERNEL DRIVER)
sto:
                    Error Control
                                    = 0x1 (SERVICE ERROR NORMAL)
sto:
                    Image Path
                                     = \SystemRoot\system32\drivers\amdk8.sys
sto:
                    Display Name
                                     = AMD K8 Processor Driver
sto:
                    Load Order Group = Extended Base
                    {Add Service Event Log: AmdK8}
sto:
                         Added 'AmdK8' entry to 'System' service event log.
sto:
                    {Add Service Event Log: exit(0x00000000)}
sto:
                    {Add Registry Key}
sto:
                         Key Path = HKLM\System\CurrentControlSet\Services\EventLog\System\AmdK8
                         Value Name = EventMessageFile
                                  = 0x00020000
                                   = "%SystemRoot%\System32\IoLogMsg.dll;%SystemRoot%\System32\drivers\amdk8.sys"
                         Value
                    {Add Registry Key: exit(0x00000000)}
                    {Add Registry Key}
                         Key Path = HKLM\System\CurrentControlSet\Services\EventLog\System\AmdK8
sto:
sto:
                         Value Name = TypesSupported
                                   = 0x00010001
sto:
                         Flags
                         Value
                                    = 7
sto:
sto:
                     Add Registry Key:
               {Add Service: exit(0x00000000)}
sto:
               {Copy File: amdk8.sys}
sto:
                    {FILE_QUEUE_COPY}
flq:
fla:
```

以及 AmdPPM 服务和 amdppm.sys 驱动。

```
{Add Service: AmdPPM}
sto:
                    Opdating existing service 'AmdPPM'.
                    Start Type
                                    = 0x3 (SERVICE DEMAND START)
sto:
                                     = 0x1 (SERVICE_KERNEL_DRIVER)
sto:
                    Service Type
                                   = 0x1 (SERVICE_ERROR_NORMAL)
sto:
                    Error Control
sto:
                   Image Path
                                     = \SystemRoot\system32\drivers\amdppm.sys
sto:
                    Display Name
                                     = AMD 处理器驱动程序
                   Load Order Group = Extended Base
sto:
                    {Add Service Event Log: AmdPPM}
sto:
                        Added 'AmdPPM' entry to 'System' service event log.
sto:
sto:
                    {Add Service Event Log: exit(0x00000000)}
                    {Add Registry Key}
sto:
                         Key Path = HKLM\System\CurrentControlSet\Services\EventLog\System\AmdPPM
sto:
                         Value Name = EventMessageFile
sto:
                                   = 0x00020000
sto:
                         Flags
                                    = "%SystemRoot%\System32\IoLogMsg.dll;%SystemRoot%\System32\drivers\amdppm.sys"
sto:
                         Value
sto:
                    {Add Registry Key: exit(0x00000000)}
                    {Add Registry Key}
sto:
                         Key Path = HKLM\System\CurrentControlSet\Services\EventLog\System\AmdPPM
                         Value Name = TypesSupported
sto:
                                   = 0x00010001
sto:
                         Flags
sto:
                         Value
                                    = 7
sto:
                     {Add Registry Key: exit(0x00000000)}
sto:
               {Add Service: exit(0x00000000)}
               {Copy File: amdppm.sys}
sto:
                    {FILE QUEUE COPY}
fla:
flq:
                         CopyStyle
                                       - 0x09000000
flq:
                         SourceRootPath - 'C:\Windows\System32\DriverStore\FileRepository\cpu.inf_amd64_neutral_f7d27831flab9185\'
                         SourceFilename - 'amdppm.sys'
flq:
                         TargetDirectory- 'C:\Windows\system32\drivers'
flq:
flq:
                         TargetFilename - 'amdppm.sys'
```

下一步计划:

请调整 TMS 策略,允许 C:\Windows\servicing\TrustedInstaller.exe 应用修改、更新以下注册表项中的内容。

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AmdK8

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AmdPPM

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\intelppm

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Processor

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ViaC7

并允许将驱动 amdk8.sys、amdppm.sys、intelppm.sys、processor.sys、viac7.sys 复制到 C:\Windows\system32\drivers\目录。

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9月10日14:32

收件人: ICBC 案例通知 < win10sup@sdc.icbc.com.cn > **抄送:** ICBC_Notification < ICBC_Notification@cmgos.com >

主题: 回复: [案例号: CAS-12143-P0Y2F1] % |P2||CBC|工行用户反馈 Win7 系统补丁安装失

败问题 % 初次响应 CMIT:0001339

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 win7 系统安装补丁 KB4474419 失败,在安装完成重启系统时进度显示 9%左右时重启回滚,但是卸载 TMS 后可以正常安装补丁,需要 CMIT 协助排查导致补丁安装失败的根本原因。

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。

您提供的日志已经收到,正在排查问题,有任何进展会及时与您沟通、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 9 月 10 日 13:14

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

抄送: Wei Liang <weiliang@cmgos.com>

主题: [案例号: CAS-12143-P0Y2F1] % |P2||CBC|工行用户反馈 V2022-L 版本系统 8 月补丁

安装失败问题 % 初次响应 CMIT:0001339

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-12143-P0Y2F1 与我联系。

如果您有任何其他疑问, 请随时与我联系。

此致,

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"。