许先生，您好：

如刚才电话沟通，鉴于当前 case 与第三方应用有关，经您的同意，此 case 做归档处理，以下为案例总结，请您知悉：

Case No：CAS-06686-V8Q9W1

问题描述：

==========

用户反馈补丁 KB5016623 安装失败。

问题分析：

==========

用户上传日志均已分析完毕并解决，其中湖北分行所上报的 access denied 问题与第三方 TMS 有关（详情可参见以往邮件），需要由第三方进行处理。

问题总结：

==========

经用户确认，用户暂时无后续需求，可归档该案例。

以上为此问题的案例总结，如有任何问题，可随时与我们联系，谢谢

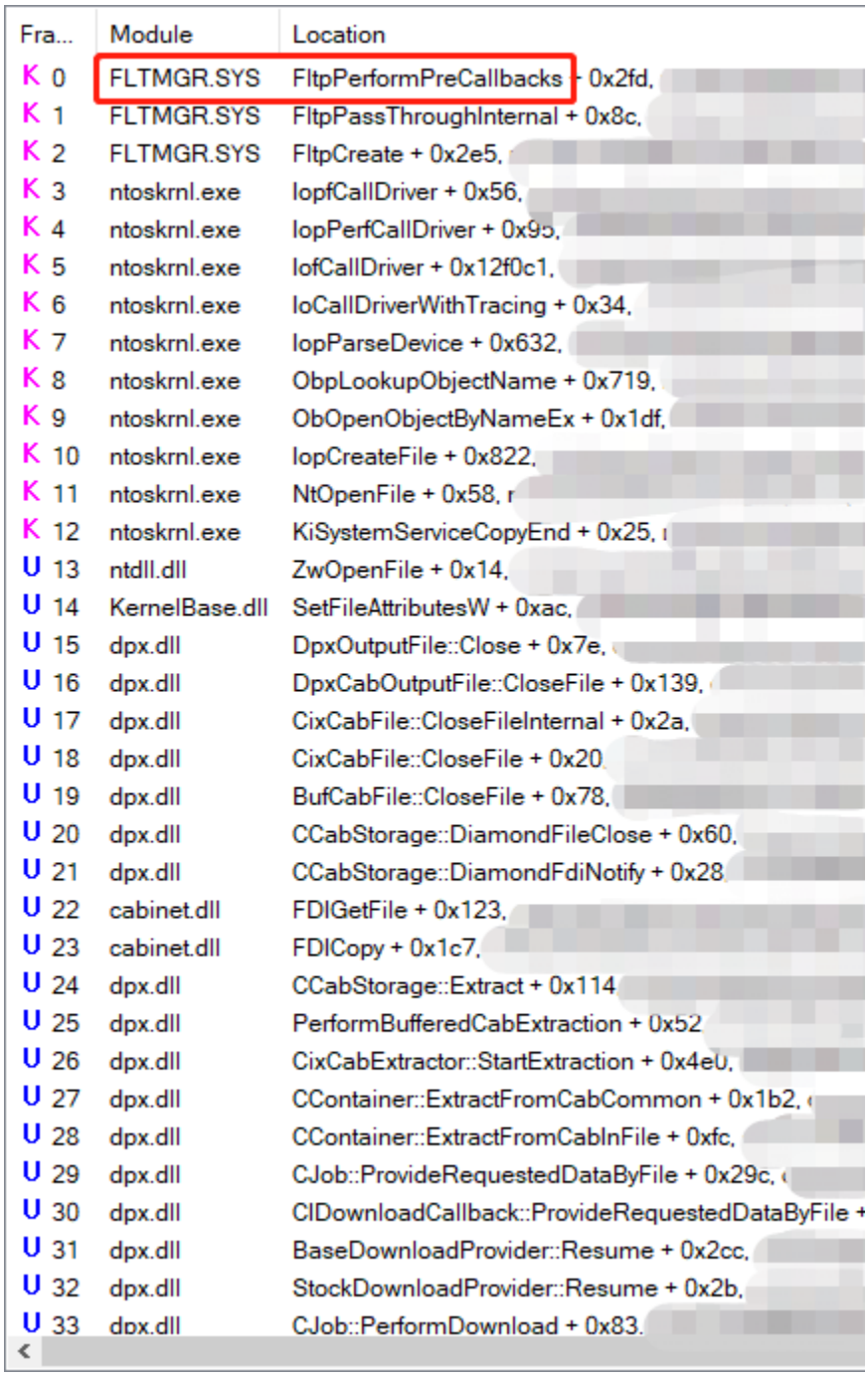
李琦 Li Qi
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话： 4008180055
电子邮箱 Email: liqi@cmgos.com

神州网信 CMIT

发件人: Li Qi
发送时间: 2022 年 9 月 28 日 16:40
收件人: '许翔' <windowsserversupport@sdc.icbc.com.cn>
抄送: 'B166ER' <939002194@qq.com>; ICBC_Notification <ICBC_Notification@cmgos.com>; 'win10 技术支持' <win10sup@sdc.icbc.com.cn>
主题: 回复： [案例号: CAS-06686-V8Q9W1] % |P2||ICBC|反馈 win10 无法安装 KB5014692 % 初次响应 CMIT:0001543

许先生，您好:

有关 access denied 的补丁安装失败问题，在上一次的日志中我们进行了进一步的排查，该问题本质是 filter driver 导致的 access denied 问题，这一点从前几次的 procmon 日志中可以看到，filter driver 在 minifilter 层抛出 access denied 的问题，但 Procom 记录到 callbacks 之后就没有更多内容，因此无法确认是具体的哪一个 filter driver。



Fra...	Module	Location
K 0	FLTMGR.SYS	FltpPerformPreCallbacks + 0x2fd,
K 1	FLTMGR.SYS	FltpPassThroughInternal + 0x8c,
K 2	FLTMGR.SYS	FltpCreate + 0x2e5,
K 3	ntoskrnl.exe	IopfCallDriver + 0x56,
K 4	ntoskrnl.exe	IopPerfCallDriver + 0x95,
K 5	ntoskrnl.exe	IofCallDriver + 0x12f0c1,
K 6	ntoskrnl.exe	IoCallDriverWithTracing + 0x34,
K 7	ntoskrnl.exe	IopParseDevice + 0x632,
K 8	ntoskrnl.exe	ObpLookupObjectName + 0x719,
K 9	ntoskrnl.exe	ObOpenObjectByNameEx + 0x1df,
K 10	ntoskrnl.exe	IopCreateFile + 0x822,
K 11	ntoskrnl.exe	NtOpenFile + 0x58, r
K 12	ntoskrnl.exe	KiSystemServiceCopyEnd + 0x25,
U 13	ntdll.dll	ZwOpenFile + 0x14,
U 14	KernelBase.dll	SetFileAttributesW + 0xac,
U 15	dpx.dll	DpxOutputFile::Close + 0x7e,
U 16	dpx.dll	DpxCabOutputFile::CloseFile + 0x139,
U 17	dpx.dll	CixCabFile::CloseFileInternal + 0x2a,
U 18	dpx.dll	CixCabFile::CloseFile + 0x20,
U 19	dpx.dll	BufCabFile::CloseFile + 0x78,
U 20	dpx.dll	CCabStorage::DiamondFileClose + 0x60,
U 21	dpx.dll	CCabStorage::DiamondFdiNotify + 0x28,
U 22	cabinet.dll	FDIGetFile + 0x123,
U 23	cabinet.dll	FDICopy + 0x1c7,
U 24	dpx.dll	CCabStorage::Extract + 0x114
U 25	dpx.dll	PerformBufferedCabExtraction + 0x52
U 26	dpx.dll	CixCabExtractor::StartExtraction + 0x4e0,
U 27	dpx.dll	CContainer::ExtractFromCabCommon + 0x1b2,
U 28	dpx.dll	CContainer::ExtractFromCabInFile + 0xfc,
U 29	dpx.dll	CJob::ProvideRequestedDataByFile + 0x29c,
U 30	dpx.dll	CIDownloadCallback::ProvideRequestedDataByFile +
U 31	dpx.dll	BaseDownloadProvider::Resume + 0x2cc,
U 32	dpx.dll	StockDownloadProvider::Resume + 0x2b,
U 33	dpx.dll	CJob::PerformDownload + 0x83,

之后我们收取了 WPR log，从当前收集的两次 wpr 来看，并没有完整记录问题发生时间点的数据。

不过，结合补丁的 CBS 安装过程，tiworker 在执行解压 cab 文件时，会将对应文件放至临时目录 C:\Windows\SoftwareDistribution\Download 下，问题也是发生在该文件夹内。因此继续查

询有关该文件夹内所有相关 cab 解压文件的 IO 记录，可以看到 filter driver 的 callbacks 操作的执行情况，其中有经过 gscfmgr.sys。

558	C:\Windows\SoftwareDistribution\Download\126a776ddc6e3f4a95f92e499e810bce\inst_Windows10.0-KB5016623-x64.cab_\x86_microsoft-windows-p..inscripts.resources_31bf3856ad364e35_10.0.17763.107_sv-se_0ca08ff661a89b17\f					17.400	12		12	696.11642020	696.11645420
559	C:\Windows\SoftwareDistribution\Download\126a776ddc6e3f4a95f92e499e810bce\inst_Windows10.0-KB5016623-x64.cab_\x86_microsoft-windows-p..inscripts.resources_31bf3856ad364e35_10.0.17763.107_sv-se_0ca08ff661a89b17\r					16.500	11		11	696.11653760	696.11656660
560	C:\Windows\SoftwareDistribution\Download\126a776ddc6e3f4a95f92e499e810bce\inst_Windows10.0-KB5016623-x64.cab_\x86_microsoft-windows-p..inscripts.resources_31bf3856ad364e35_10.0.17763.107_tr-tr_b5adda3d50649d08\f					34.400	11		11	696.11666080	696.11670710
561	C:\Windows\SoftwareDistribution\Download\126a776ddc6e3f4a95f92e499e810bce\inst_Windows10.0-					19.2	12		12	696.11677	696.11680

	KB5016623-x64.cab_\x86_microsoft-windows-p..inscripts.resources_31bf3856ad364e35_10.0.17763.107_tr-tr_b5adda3d50649d08\r						00			4100	5600
562		4	System	500	[Root]		17.800	8		8	696.11677850 0	696.11680560 0
563					ntoskrnl.exe!KxStartSystemThread		17.800	8		8	696.11677850 0	696.11680560 0
564					ntoskrnl.exe!PspSystemThreadStartup		17.800	8		8	696.11677850 0	696.11680560 0
565					ntoskrnl.exe!ExpWorkerThread		17.800	8		8	696.11677850 0	696.11680560 0
566					ntoskrnl.exe!CcWriteBehindInternal		17.800	8		8	696.11677850 0	696.11680560 0

567					ntoskrnl.exe!CcDeleteSharedCacheMap		17.800	8		8	696.11677850	696.11680560
568					ntoskrnl.exe!ObfDereferenceObject		17.800	8		8	696.11677850	696.11680560
569					ntoskrnl.exe!ObpRemoveObjectRoutine		17.800	8		8	696.11677850	696.11680560
570					|-ntoskrnl.exe!IopDeleteFile		7.200	4		4	696.11679780	696.11680560
571					| ntoskrnl.exe!IofCallDriver		7.200	4		4	696.11679780	696.11680560
572					| ntoskrnl.exe!IopPerfCallDriver		7.200	4		4	696.11679780	696.11680560
573					| ntoskrnl.exe!IopfCallDriver		7.200	4		4	696.11679780	696.11680560

574					| FLTMGR.SYS!FltpDispatch		7.2000	4		4	696.11679780 0	696.11680560 0
575					| FLTMGR.SYS!FltpPassThrough		7.2000	4		4	696.11679780 0	696.11680560 0
576					| FLTMGR.SYS!FltpPassThroughInternal		7.2000	4		4	696.11679780 0	696.11680560 0
577					| FLTMGR.SYS!FltpPerformPreCallbacks		7.2000	4		4	696.11679780 0	696.11680560 0
578					| FLTMGR.SYS!FltpPerfTraceOperationCallback		7.2000	4		4	696.11679780 0	696.11680560 0
579					|	PROCMON24.SYS	1.5000	1	0xFFFF91031B8FA010	1	696.11679780 0	696.11679930 0
580					|	fileinfo.sys	2.8000	1	0xFFFF91031B8FA010	1	696.11680280 0	696.11680560 0
581					|	gscfmg	1.6	1	0xFFFF91031B	1	696.11679	696.11680

					r.sys	00		8FA010		9500	1100	
582				|	TmPreFlt.sys	1.300	1	0xFFFF91031B8FA010	1	696.11680130 0	696.11680260 0	
583				|- ntoskrnl.exe!MiSectionDelete		10.6000	4		4	696.11677850 0	696.11678970 0	
584				| ntoskrnl.exe!MiDereferenceControlAreaBySection		10.6000	4		4	696.11677850 0	696.11678970 0	
585				| ntoskrnl.exe!MiCheckControlArea		10.6000	4		4	696.11677850 0	696.11678970 0	
586				| ntoskrnl.exe!MiSegmentDelete		10.6000	4		4	696.11677850 0	696.11678970 0	
587				| ntoskrnl.exe!ObfDereferenceObject		10.6000	4		4	696.11677850 0	696.11678970 0	

588					| ntoskrnl.exe!ObpRemoveObjectRoutine		10.6000	4		4	696.11677850 0	696.11678970 0
589					| ntoskrnl.exe!IopDeleteFile		10.6000	4		4	696.11677850 0	696.11678970 0
590					| ntoskrnl.exe!IofCallDriver		10.6000	4		4	696.11677850 0	696.11678970 0
591					| ntoskrnl.exe!IopPerfCallDriver		10.6000	4		4	696.11677850 0	696.11678970 0
592					| ntoskrnl.exe!IopfCallDriver		10.6000	4		4	696.11677850 0	696.11678970 0
593					| FLTMGR.SYS!FltpDispatch		10.6000	4		4	696.11677850 0	696.11678970 0

594					| FLTMGR.SYS!FltpPassThrough		10.6000	4		4	696.11677850 0	696.11678970 0
595					| FLTMGR.SYS!FltpPassThroughInternal		10.6000	4		4	696.11677850 0	696.11678970 0
596					| FLTMGR.SYS!FltpPerformPreCallbacks		10.6000	4		4	696.11677850 0	696.11678970 0
597					| FLTMGR.SYS!FltpPerfTraceOperationCallback		10.6000	4		4	696.11677850 0	696.11678970 0
598					|	PROCMON24.SYS	2.6000	1	0xFFFF91031B8FA010	1	696.11677850 0	696.11678110 0
599					|	fileinfo.sys	3.6000	1	0xFFFF91031B8FA010	1	696.11678610 0	696.11678970 0
600					|	gscfmgr.sys	2.4	1	0xFFFF91031B	1	696.11678	696.11678

							00		8FA010		1300	3700
601						TmPreFlt.sys	2.000	1	0xFFFF91031B8FA010	1	696.11678390 0	696.11678590 0

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: 2022 年 9 月 20 日 10:32
收件人: 'B166ER' <939002194@qq.com>
主题: 回复: 回复： [案例号: CAS-06686-V8Q9W1] % |P2||ICBC|反馈 win10 无法安装 KB5014692 % 初次响应 CMIT:0001543

刘先生，您好：

好的，可以的。

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: B166ER <939002194@qq.com>
发送时间: 2022 年 9 月 20 日 10:30
收件人: Li Qi <liqi@cmgos.com>
主题: 回复： [案例号: CAS-06686-V8Q9W1]％ |P2||ICBC|反馈 win10 无法安装 KB5014692 ％初次响应 CMIT:0001543

您好，最近几天有考核，日志缓两天再取可否？？:)

---原始邮件---
发件人: "liqi"<liqi@cmgos.com>
发送时间: 2022 年 9 月 20 日(周二) 上午 9:41
收件人:
"windowsserversupport"<windowsserversupport@sdc.icbc.com.cn>;"939002194"<939002194@qq.com>;
抄送: "ICBC_Notification"<ICBC_Notification@cmgos.com>;"win10sup"<win10sup@sdc.icbc.com.cn>;
主题: 回复：［案例号: CAS-06686-V8Q9W1 ］％ |P2||ICBC|反馈 win10 无法安装 KB5014692 ％ 初次响应 CMIT:0001543

刘先生，您好：

如刚才电话沟通，在查看您本次上传的 wpr+procmon 日志时发现，记录的抓取过程中由于本地有缓存记录，因此未能捕获到 filter driver 对更新过程的干预。因此需要您将 c:\windows\softwaredistribution 文件夹重命名后重新抓取 wpr+procmon。

当前问题经您的本地测试，在禁用 TMS 情况下，补丁可以正常安装。从之前的日志中得出的结论为 C:\Windows\SoftwareDistribution\Download\126a776ddc6e3f4a95f92e499e810bce\inst_Windows10.0-KB5016623-x64.cab_\amd64_dual_wpdmtp.inf_31bf3856ad364e35_10.0.17763.1697_none_f3f3f27a8f89a4d0\r\wpdmtp.dll 导致的 access denied 问题。因此合理怀疑为 filter driver 对补丁文件的安装过程造成了干预。目前尝试通过在抓取日志中查看 filter driver 对问题文件的 handle 记录。但从日志中找到 filter driver 干预的证据难度较大，很有可能无法看到相关进程记录。因此还请协助将本地缓存清理后再收取一遍上述日志。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

发件人: Wei Liang <weiliang@cmgos.com>
发送时间: 2022 年 9 月 2 日 17:56
收件人: 许翔 <windowsserversupport@sdc.icbc.com.cn>; B166ER <939002194@qq.com>; Li Qi <liqi@cmgos.com>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>; win10 升级支持 <win10sup@sdc.icbc.com.cn>
主题: 回复: 回复： [案例号: CAS-06686-V8Q9W1] % |P2||ICBC|反馈 win10 无法安装 KB5014692 % 初次响应 CMIT:0001543

许先生 您好：

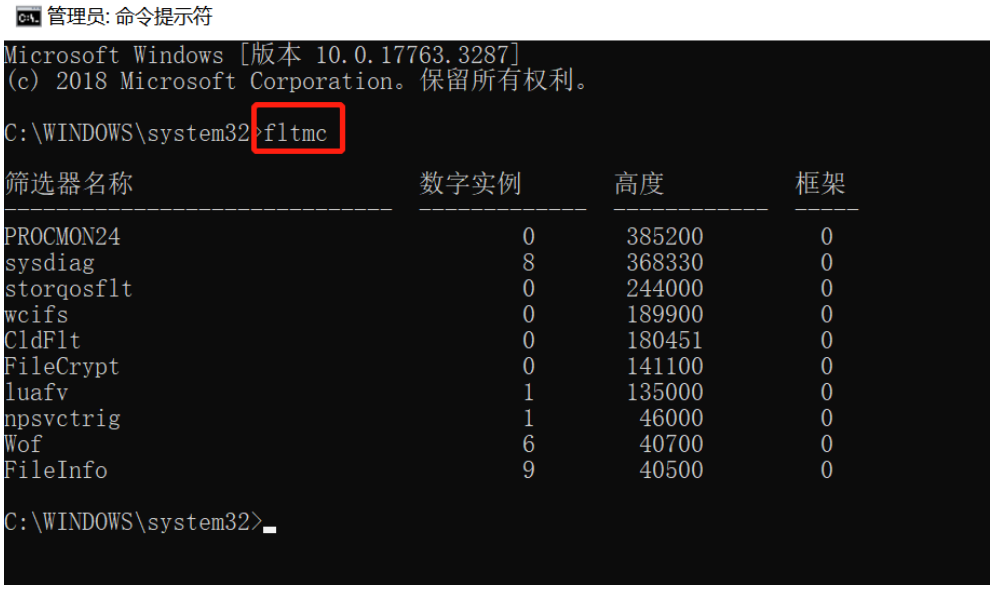
感谢您的电话接听。

如上一封邮件所说，当脱管 TMS 后，补丁可以正常安装。因此有关 access denied 的错误，当前合理怀疑为由第三方应用的干预导致。

目前从 procmon 里面看不到具体哪个 filter driver 导致 access denied 的问题，接下来我们会尝试同时抓取 wpr+procmon，看能否找到具体的问题点。

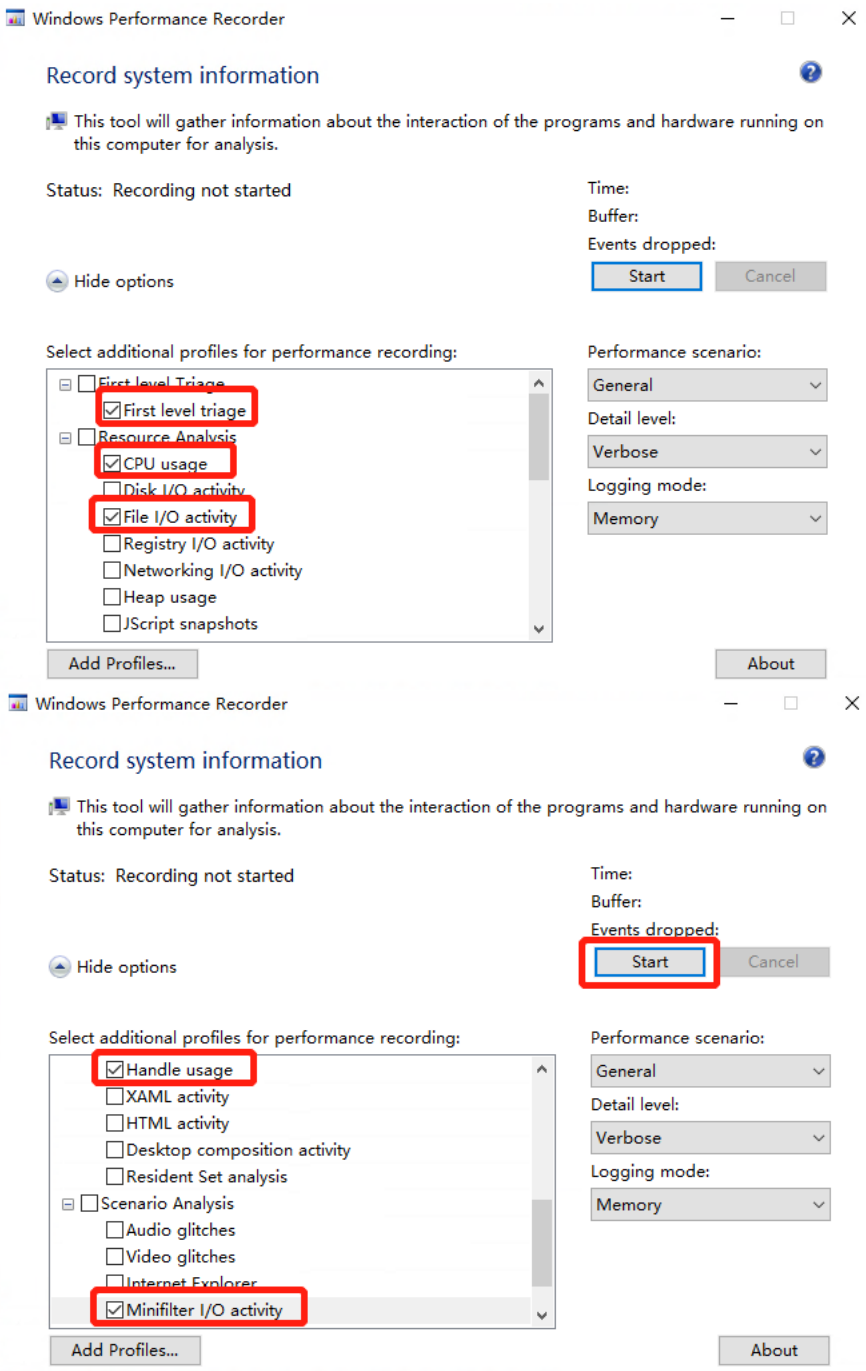
请按照以下操作获取相关信息并通过 sftp 或 CDUC 上传。

1）在出现补丁更新失败报 0x80070005 错误的设备上，以**管理员权限**打开 cmd 命令行，执行 **fltmc** 命令，查看对应的 filter driver，**并提供此截图。**（如下图所示）

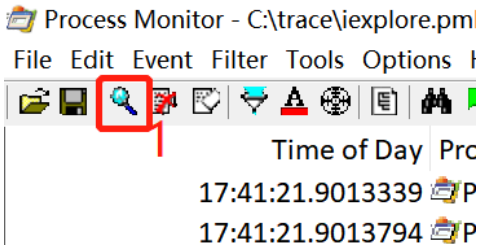


2）下载附件中的 **wpr.zip、procmon.zip 和 CMGELogCollector.zip** 工具，解压后复制到问题设备上。

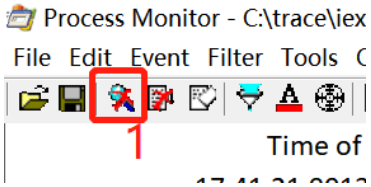
3）打开 wpr 目录，运行 wprui.exe，按照下图所示配置，即勾选 **“First level triage”、“CPU usage”、“File I/O activity”、“Handle usage”、“Minifilter I/O activity”** 后，点击 **“Start”** 开始抓取 wpr 日志。

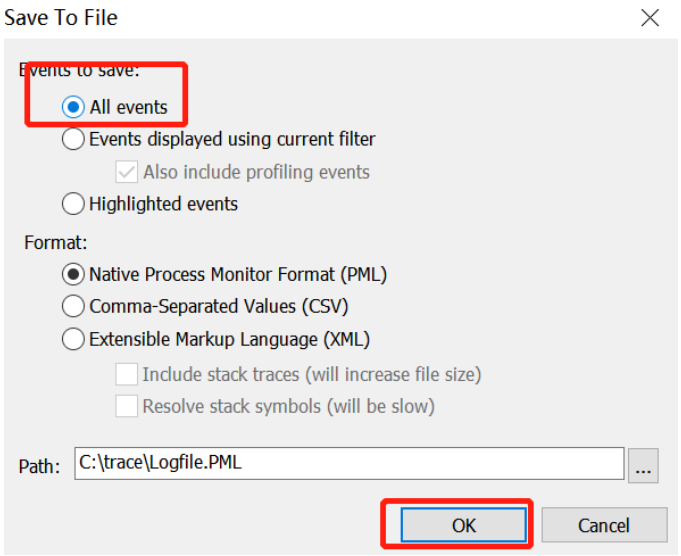


4）运行 procmon.exe，点击 accept 后，到达如下图的界面：（图标 1 不带 x 表示处于抓取状态）



5）**此时离线安装 KB5016623 更新补丁，**待提示安装失败，复现问题后，点击图标 1 停止抓取（停止抓取后图标 1 带 x），点击“ “File”-“save”，选择 all events 保存 pml 文件，将**此文件压缩后上传**。





6）回到 wprui 界面，点击“Save”保存，指定目录保存 wpr 日志，将 **wpr 日志压缩后上传**。

7）将 C:\Windows\SysWOW64\Pclient\logs **目录压缩后上传**。

8）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，将日志上传**。

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

神州网信 CMIT

发件人： Li Qi <liqi@cmgos.com>
发送时间： 2022 年 8 月 30 日 16:33
收件人： 许翔 <windowsserversupport@sdc.icbc.com.cn>
抄送： ICBC_Notification <ICBC_Notification@cmgos.com>; win10 升级支持 <win10sup@sdc.icbc.com.cn>; B166ER <939002194@qq.com>
主题： 回复： [案例号: CAS-06686-V8Q9W1] % |P2||ICBC|反馈 win10 无法安装 KB5014692 % 初次响应 CMIT:0001543

许先生，您好：

如刚才电话沟通，目前针对湖北分行出现的补丁更新失败问题，有如下分析，供您参考：

1. 更新失败的错误为 0x80070005，意为：access denied。从直接报错来看，受权限不足导致的操作失败。

```
# for hex 0x80070005 / decimal -2147024891
  COR_E_UNAUTHORIZEDACCESS                                  corerror.h
# Access is denied.
  DIERR_OTHERAPPHASPRIO                                     dinput.h
  DIERR_READONLY                                            dinput.h
  DIERR_HANDLEEXISTS                                        dinput.h
  DSERR_ACCESSDENIED                                        dsound.h
  STIERR_READONLY                                           stierr.h
  STIERR_NOTINITIALIZED                                     stierr.h
  E_ACCESSDENIED                                            winerror.h
# General access denied error
# as an HRESULT: Severity: FAILURE (1), FACILITY_WIN32 (0x7), Code 0x5
# for hex 0x5 / decimal 5
  ERROR_ACCESS_DENIED                                       winerror.h
# Access is denied.
# 9 matches found for "0x80070005"
```

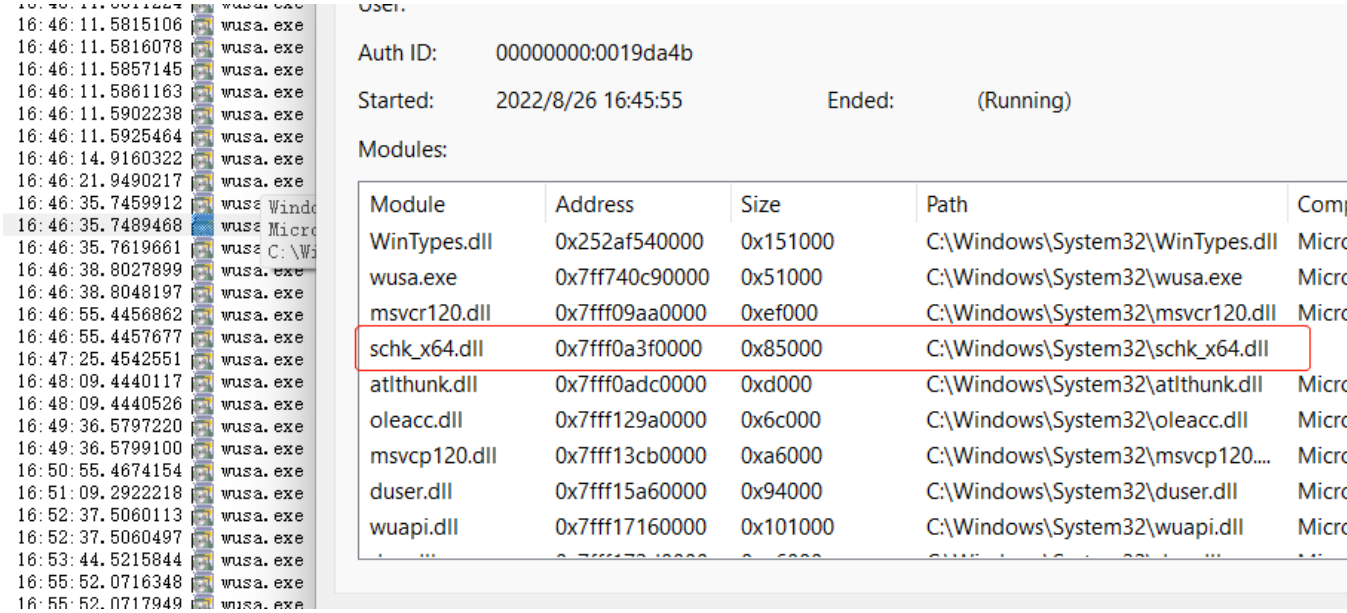
2. 结合用户提供的 procmon 日志和 CBS 日志来看，出现问题的文件为：C:\Windows\SoftwareDistribution\Download\126a776ddc6e3f4a95f92e499e810bce\inst_Windows10.0-KB5016623-x64.cab_\amd64_dual_wpdmtp.inf_31bf3856ad364e35_10.0.17763.1697_none_f3f3f27a8f89a4d0\r\wpdmtp.dll

```
16:50:46.9908730  TiWorker.exe   6976  ReadFile        C:\Windows\SoftwareDistribution\Download\126a776ddc6e3f4a95
16:50:46.9909553  TiWorker.exe   6976  CreateFile      C:\Windows\SoftwareDistribution\Download\126a776ddc6e3f4a95
16:50:46.9910216  TiWorker.exe   6976  QueryBasicIn... C:\Windows\SoftwareDistribution\Download\126a776ddc6e3f4a95
16:50:46.9910278  TiWorker.exe   6976  CloseFile       C:\Windows\SoftwareDistribution\Download\126a776ddc6e3f4a95
16:50:46.9910871  TiWorker.exe   6976  CreateFile      C:\Windows\SoftwareDistribution\Download\126a776ddc6e3f4a95
16:50:46.9922414  TiWorker.exe   6976  QueryBasicIn... C:\Windows\SoftwareDistribution\Download\126a776ddc6e3f4a95
16:50:46.9922714  TiWorker.exe   6976  QuerySecurit... C:\Windows\SoftwareDistribution\Download\126a776ddc6e3f4a95
16:50:46.9922836  TiWorker.exe   6976  SetEndOfFile... C:\Windows\SoftwareDistribution\Download\126a776ddc6e3f4a95
16:50:46.9923415  TiWorker.exe   6976  SetAllocatio... C:\Windows\SoftwareDistribution\Download\126a776ddc6e3f4a95
16:50:46.9923621  TiWorker.exe   6976  WriteFile       C:\Windows\SoftwareDistribution\Download\126a776ddc6e3f4a95
16:50:46.9923954  TiWorker.exe   6976  SetEndOfFile... C:\Windows\SoftwareDistribution\Download\126a776ddc6e3f4a95
16:50:46.9924325  TiWorker.exe   6976  SetAllocatio... C:\Windows\SoftwareDistribution\Download\126a776ddc6e3f4a95
16:50:46.9924476  TiWorker.exe   6976  SetBasicInfo... C:\Windows\SoftwareDistribution\Download\126a776ddc6e3f4a95
16:50:46.9925017  TiWorker.exe   6976  CreateFile      C:\Windows\SoftwareDistribution\Download\126a776ddc6e3f4a95
16:50:46.9925844  TiWorker.exe   6976  CreateFile      amd64_dual_wpdmtp.inf_31bf3856ad364e35_10.0.17763.1697_none
16:50:46.9930898  TiWorker.exe   6976  QueryAttribu... C:\Windows\SoftwareDistribution\Download\126a776ddc6e3f4a95
16:50:46.9931010  TiWorker.exe   6976  QueryBasicIn... C:\Windows\SoftwareDistribution\Download\126a776ddc6e3f4a95
16:50:46.9931402  TiWorker.exe   6976  CreateFile      C:\Windows\SoftwareDistribution\Download\126a776ddc6e3f4a95
16:50:46.9931813  TiWorker.exe   6976  CloseFile       C:\Windows\SoftwareDistribution\Download\126a776ddc6e3f4a95
16:50:46.9932619  TiWorker.exe   6976  QueryStandar... C:\Windows\Logs\CBS\CBS.log
16:50:46.9932704  TiWorker.exe   6976  WriteFile       C:\Windows\Logs\CBS\CBS.log
```

3. 补丁更新过程为：wusa 进程将 msu 文件解压为 cab 文件，使用 cab 文件中包含的 TiWorker.exe 进行系统组件的更新与替换。其中上述路径即为补丁安装过程

中 cab 文件解压至本地的临时路径，补丁安装的正常情况下，解压至 SoftwareDistribution 文件夹后，会将对应的 windows 组件拷贝至系统的 winsxs 文件夹中完成 CBS 安装，但在解压至临时路径时出现 access denied 的错误，中断安装过程。

4. 从用户的实际测试反馈来看，当托管 TMS 后，补丁可以正常安装。因此有关 access denied 的错误，当前合理怀疑为由第三方应用的干预导致。相关可参考的证据包括，补丁安装最开始阶段，wusa 进程有 schk_x64.dll 的参与。其他关联证据正在继续分析中。



以上，如有进一步进展，会第一时间向您更新，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

发件人：Li Qi
发送时间：2022 年 8 月 24 日 15:44
收件人：’许翔’<windowsserversupport@sdc.icbc.com.cn>
抄送：ICBC_Notification <ICBC_Notification@cmgos.com>; ’win10 升级支持’ <win10sup@sdc.icbc.com.cn>
主题：回复: 回复： [案例号: CAS-06686-V8Q9W1] % |P2||ICBC|反馈 win10 无法安装 KB5014692 % 初次响应 CMIT:0001543

许先生，您好：

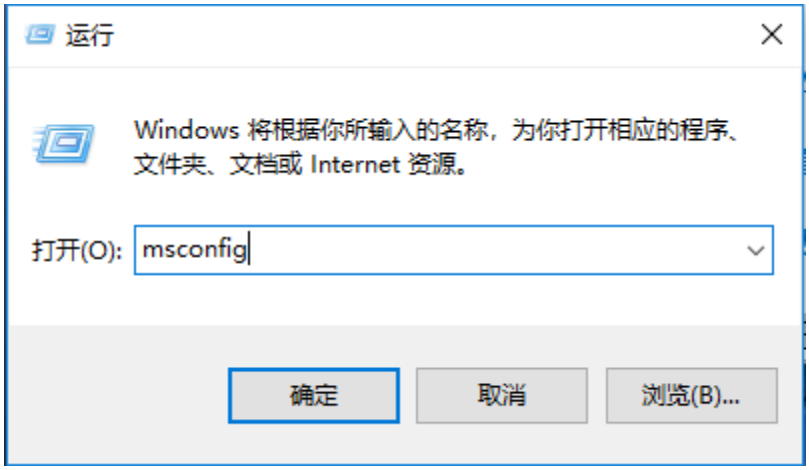
如刚才电话沟通，有关近期出现 ACCESSDENIED 报错的更新失败问题，需要用户尝试如下操作：

1， clean boot：

在运行栏内输入 msconfig，调出系统配置，在“常规”下选择“有选择的启动”，勾选加载系统服务和加载启动项。在“服务”选项下，勾选“隐藏所有 Microsoft 服务”，再点击“全部禁用”-确定，重启进入 Clean boot。

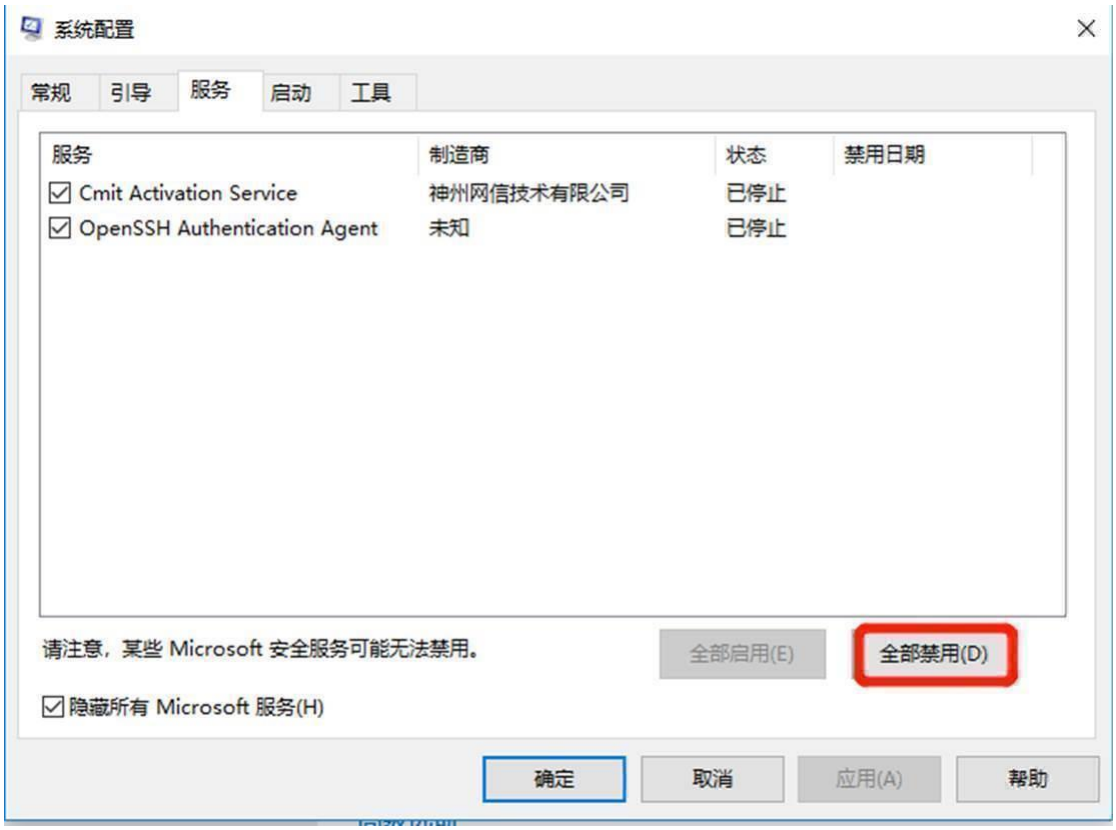
步骤操作：

- 在运行栏内输入 msconfig，调出系统配置



- 在“常规”选项下选择“有选择的启动”，勾选加载系统服务和加载启动项

- 在“服务”选项下，勾选“隐藏所有 Microsoft 服务”，再点击“全部禁用”-确定

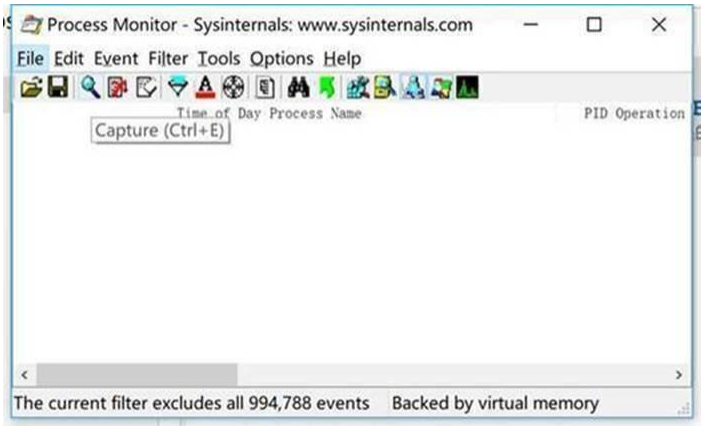


- 重启进入 Clean boot
- 手动离线安装 KB5015811

2， 收取 procmon：

如 clean boot 仍然安装失败，则需要收集 Procmon 日志，Procmon 收集方法如下：

1) 保存附件 processmonitor.zip 至本地计算机
2) 解压完成后，双击执行 procmon.exe
3) 显示如下界面，并点击 capture 按钮，先暂停收集，准备进行捕获
4) 点击 clear 按钮，清空当前窗口，然后点击 capture 按钮，开始捕获

5) 

6) 进行离线安装，待问题复现后（即安装失败出现报错信息），再次点击 capture 按钮，停止捕获

7) 点击 File menu，点击 Save. 选择"All events" and "Native Process Monitor Format (PML)"点击 OK，并将此文件回传给我进行分析，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

发件人：Li Qi
发送时间：2022 年 8 月 19 日 18:07
收件人：'许翔' <windowsserversupport@sdc.icbc.com.cn>
抄送：ICBC_Notification <ICBC_Notification@cmgos.com>; 'win10 升级支持' <win10sup@sdc.icbc.com.cn>

主题: 回复: 回复: [案例号: CAS-06686-V8Q9W1] % |P2||ICBC|反馈 win10 无法安装 KB5014692 % 初次响应 CMIT:0001543

许先生，您好：

如刚才电话沟通，根据您最新上传的补丁更新失败日志，可以看到如下报错：

2022-08-16 12:05:29,
Info DPX Ended DPX phase: Resume and Download Job

2022-08-16 12:05:29,
Info DPX DpxException hr=0x80070005 code=0x020217

2022-08-16 12:05:29,
Info CBS Failed to Resume job in DpxThreadResumeJobProc [HRESULT = 0x80070005 - E_ACCESSDENIED]

2022-08-16 12:05:29,
Info CBS Failed to extract files from cabinet \\?\C:\WINDOWS\SoftwareDistribution\Download\0d0a8a4c61ea8935e1c01bdac8bbb7d1\inst_Windows10.0-KB5015811-x64.cab_\Cab_3_for_KB5015811_PSFX.cab [HRESULT = 0x80070005 - E_ACCESSDENIED]

2022-08-16 12:05:29,
Info CBS Failed to extract all files from cabinet \\?\C:\WINDOWS\SoftwareDistribution\Download\0d0a8a4c61ea8935e1c01bdac8bbb7d1\inst_Windows10.0-KB5015811-x64.cab_\Cab_3_for_KB5015811_PSFX.cab [HRESULT = 0x80070005 - E_ACCESSDENIED]

2022-08-16 12:05:29,
Info CBS Failed to extract payload from cabinets [HRESULT = 0x80070005 - E_ACCESSDENIED]

2022-08-16 12:05:29,
Info CBS Failed to extract all

files from cabinet \\?\C:\WINDOWS\SoftwareDistribution\Download\0d0a8a4c61ea8935e1c01bdac8bbb7d1\inst\Windows10.0-KB5015811-x64.cab [HRESULT = 0x80070005 - E_ACCESSDENIED]

2022-08-16 12:05:29, Info CBS Failed to add package: Package_for_RollupFix~31bf3856ad364e35~amd64~~17763.3165.1.8 [HRESULT = 0x80070005 - E_ACCESSDENIED]

2022-08-16 12:05:29, Info CBS Failed to plan execution. [HRESULT = 0x80070005 - E_ACCESSDENIED]

2022-08-16 12:05:29, Error CBS Failed to process single phase execution. [HRESULT = 0x80070005 - E_ACCESSDENIED]

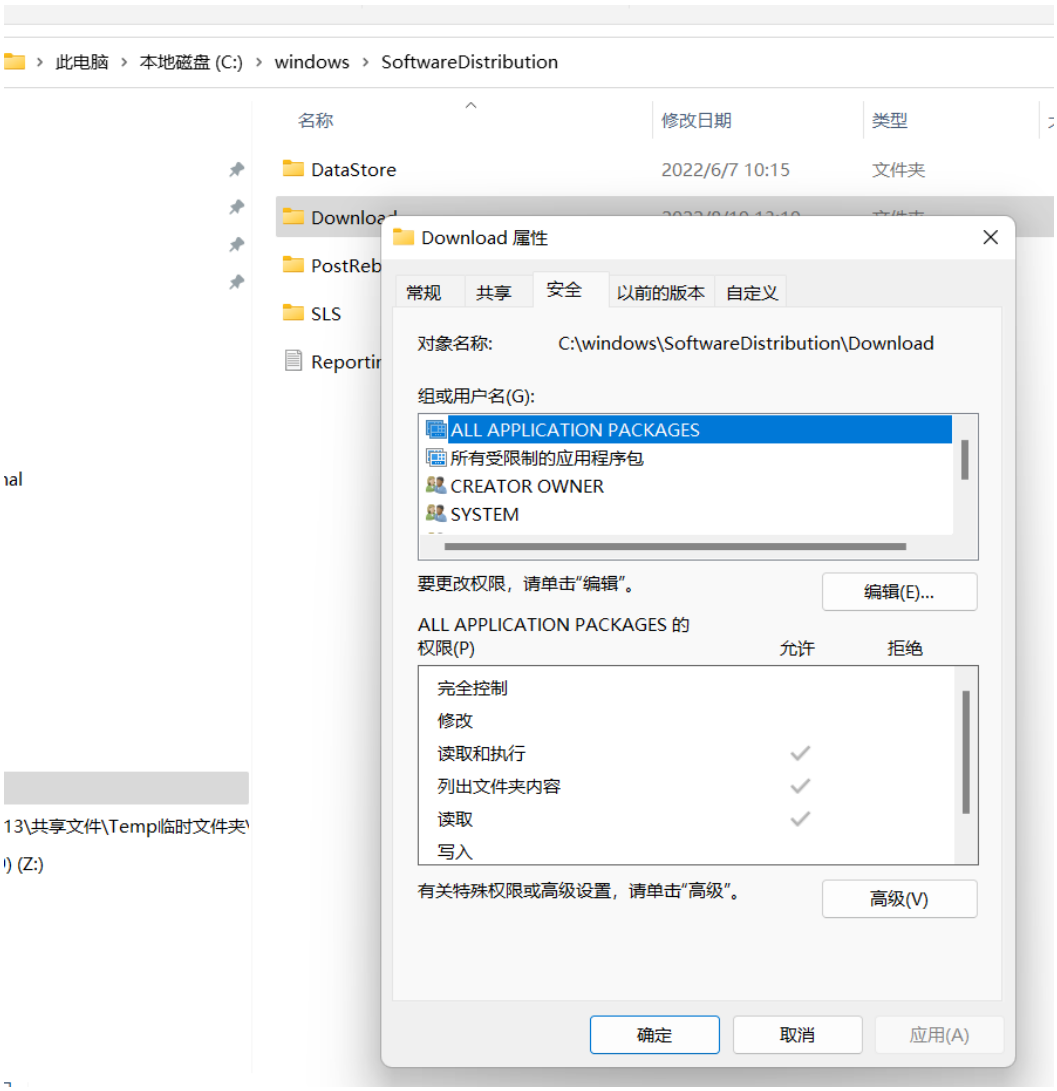
2022-08-16 12:05:29, Info CBS WER: Generating failure report for package: Package_for_ServicingStack_3100~31bf3856ad364e35~amd64~~17763.3100.1.0, status: 0x80070005, failure source: CBS Other, start state: Installed, target state: Installed, client id: WindowsUpdateAgent

2022-08-16 12:05:29, Info CBS Not able to query DisableWerReporting flag. Assuming not set... [HRESULT = 0x80070002 - ERROR_FILE_NOT_FOUND]

从日志可以看出，补丁在解压安装时出现权限不足的报错。因此安装失败。

下一步动作：

1. 请删除 c:\windows\SoftwareDistribution\Download 文件夹，由系统重新创建后尝试
2. 请离线安装 KB5015811 补丁包，下载路径为：https://support.cmgos.com/kb/5015811
3. 如 1,2 步骤失败，请截图 C:\WINDOWS\SoftwareDistribution\Download 文件夹的安全选项卡给我，如下：



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：2022 年 8 月 17 日 17:30
收件人：'许翔'<windowsserversupport@sdc.icbc.com.cn>
主题：回复：回复：［案例号：CAS-06686-V8Q9W1 ］% |P2||ICBC|反馈 win10 无法安装 KB5014692 % 初次响应 CMIT:0001543

许先生，您好：

您可以看下附件，是否说的是这个 case？

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：2022 年 8 月 15 日 13:43
收件人：'李嘉'<26239892@qq.com>
抄送：ICBC_Notification <ICBC_Notification@cmgos.com>; '许翔' <windowsserversupport@sdc.icbc.com.cn>
主题：回复：回复：［案例号：CAS-06686-V8Q9W1 ］% |P2||ICBC|反馈 win10 无法安装 KB5014692 % 初次响应 CMIT:0001543

李先生，您好：

感谢您的反馈，如后续出现类似问题可再与我联系，辛苦了。

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：李嘉 <26239892@qq.com>
发送时间：2022 年 8 月 15 日 12:53
收件人：Li Qi <liqi@cmgos.com>
主题：回复：［案例号: CAS-06686-V8Q9W1 ］% |P2||ICBC|反馈 win10 无法安装 KB5014692 % 初次响应 CMIT:0001543

经由您提供的办法修改注册表后，离线安装 6 月的累积更新成功，联机后继续安装 7 月的更新补丁也成功了，非常感谢！

发自我的 iPhone

---------- 原始邮件 ----------

发件人： Li Qi <liqi@cmgos.com>

发送时间： 2022 年 8 月 12 日 14:53

收件人： 李嘉 <26239892@qq.com>

抄送： ICBC_Notification <ICBC_Notification@cmgos.com>, 许翔 <windowsserversupport@sdc.icbc.com.cn>

主题： 回复： [案例号: CAS-06686-V8Q9W1] % |P2||ICBC|反馈 win10 无法安装 KB5014692 % 初次响应 CMIT:0001543

李先生，您好：

如刚才电话沟通，由于当前江西分行有关 6 月补丁安装失败的问题已通过重新安装，系统升级等手段进行了系统组件的修复。不再复现该问题。因此仅针对您上传的第二份日志做结果分析，如下：

根据日志显示，6 月补丁 KB5014692 通过 WSUS 进行推送安装，在 15:28 开始解压，到 15:58 提示 0x800f0821 错误。

```
2022-08-05 15:28:02, Info                                  CBS      Exec:
Extracting package:
Package_for_RollupFix~31bf3856ad364e35~amd64~~17763.3046.2.15

。。。

2022-08-05 15:58:14,
Info                                  CBS      Client aborted the
install. [HRESULT = 0x800f0821 - CBS_E_ABORT]

2022-08-05 15:58:14,
Info                                  CBS      Failed to send progress
while staging package:
Package_8309_for_KB5014692~31bf3856ad364e35~amd64~~10.0.2.15 [HRESULT =
0x800f0821 - CBS_E_ABORT]

2022-08-05 15:58:14, Error                                 CBS      Failed
to stage execution package:
```

```
Package_8309_for_KB5014692~31bf3856ad364e35~amd64~~10.0.2.15 [HRESULT =
0x800f0821 - CBS_E_ABORT]

2022-08-05 15:58:14,
Info                                  CBS      CommitPackagesState:
Started persisting state of packages

2022-08-05 15:58:14,
Info                                  CBS      CommitPackagesState:
Completed persisting state of packages
```

该问题为 known issue，其原因为 USO 有 30 分钟 timeout 的机制导致，该问题未来会在 8 月补丁中进行修复，将该 timeout 机制延长至 4 小时。理论上手动安装该补丁是不受这个 timeout 机制的影响的。您可以尝试手动安装查看是否有其他报错。

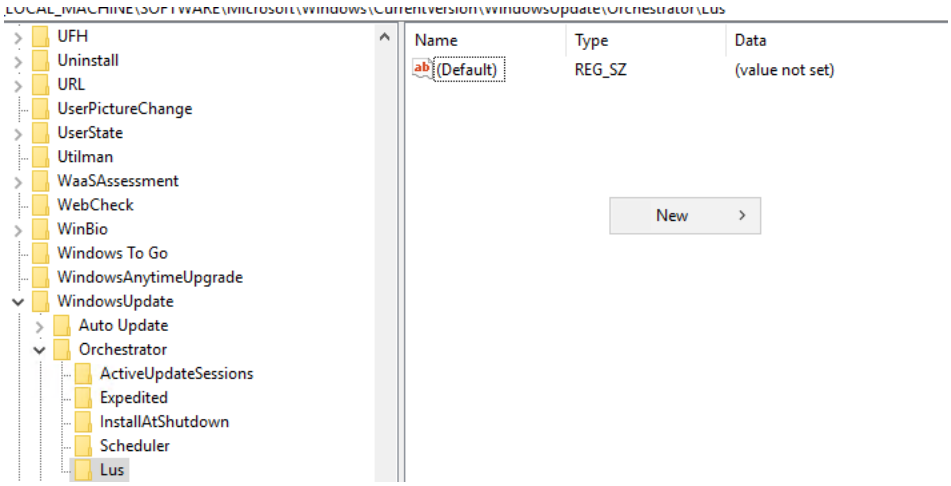
作为 workaround，您可以通过添加如下键值尝试：

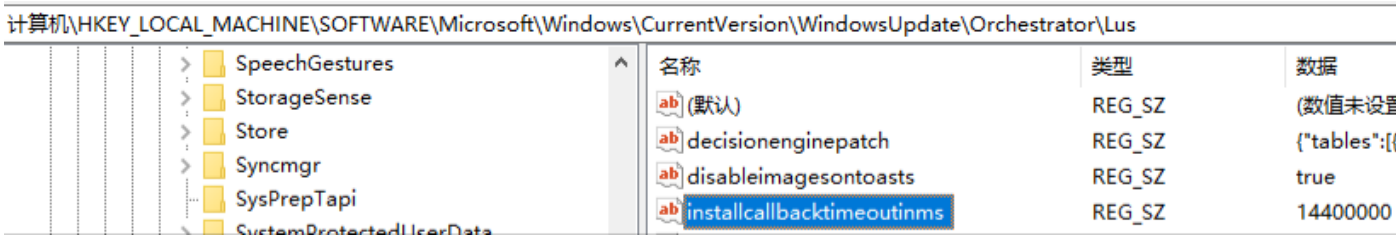
1. HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Orchestrator\Lus(如没有 Lus，请自行创建)

1 Value Name：installcallbacktimeoutinms

1 Value：14400000

1 Value Type：REG_SZ





2. 停止 Windows Update 和 Update Orchestrator Service 服务

3. 重命名 C:\Windows\SoftwareDistribution 为 SoftwareDistribution.old

4. 进行 WSUS 下载安装补丁。

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：李嘉 <26239892@qq.com>
发送时间：2022 年 8 月 11 日 11:39
收件人：Li Qi <liqi@cmgos.com>
主题：回复：回复：[案例号：CAS-06686-V8Q9W1] % |P2||ICBC|反馈 win10 无法安装 KB5014692 % 初次响应 CMIT:0001543

您好：

这是一台 dell 7070 机型的设备，我们已经采用了您之前说的指令，卸载 TMS、用 1809 版镜像重新升级等多种措施，仍然无法完成安装，附上日志，请帮忙分析原因。