许先生，您好：

如刚才电话沟通，经您的确认，当前问题已解决，此 case 将做关闭处理，以下为案例总结，请您知悉：

Case No：CAS-11631-B2M1Q8

问题描述：

==========

用户反馈安装软件失败问题，涉及 3-4 台设备，该问题在其他版本操作系统上也有出现，报错为：Swbemobiectset: 拍绝访问。需要协助分析处理。

问题分析：

==========

经日志分析，怀疑在加域以后，wmi class 权限丢失导致软件安装失败。

其核心的报错的逻辑如下：

Wbemdisp!CSWbemObjectSet::get_Count

相关日志报错显示在安装过程中的报错由 wbem 返回

9:45:31.9877779 AM 工银 e 企邮_3.0.3-877_fh_amduni.tmp 8272 9948 RegCloseKey HKLM\SOFTWARE\WOW6432Node\Microsoft\WBEM\CIMOM SUCCESS 1 INTRANET\hlfh-fujx01

9:45:31.9879243 AM 工银 e 企邮_3.0.3-877_fh_amduni.tmp 8272 9948 RegQueryKey HKCU\Software\Classes SUCCESS Query: Name 1 INTRANET\hlfh-fujx01

15	KernelBase.dll	BaseRegGetKeySemantics + 0x38, minkernel\s
16	KernelBase.dll	BaseRegOpenClassKey + 0x73, minkernel\scre
17	KernelBase.dll	BaseRegOpenKeyInternal + 0x115, minkernel\s
18	KernelBase.dll	RegOpenKeyExInternalW + 0x19e, minkernel\sc
19	KernelBase.dll	RegOpenKeyExW + 0x1c, minkernel\screg\winre
20	combase.dll	CComRegCatalog::GetClassInfoW + 0x24f, one
21	combase.dll	CComCatalog::GetClassInfoInternal + 0x10db,
22	combase.dll	CComCatalog::GetClassInfoW + 0x64, onecore\
23	combase.dll	ICoCreateInstanceEx + 0x1da, onecore\com\co
24	combase.dll	CComActivator::DoCreateInstance + 0x175, one
25	combase.dll	CoCreateInstance + 0xa7, onecore\com\combas
26	wbemdisp.dll	MapHresultToWmiDescription + 0x2a, onecore\a
27	wbemdisp.dll	CDispatchHelp::RaiseException + 0x2f, onecore
28	wbemdisp.dll	CSWbemObjectSet::get_Count + 0x13e, onecor
29	oleaut32.dll	tPushValJmpTab + 0x107, mincore\com\oleaut3
30	oleaut32.dll	CTypeInfo2::Invoke + 0x26f, mincore\com\oleau
31	wbemdisp.dll	CDispatchHelp::Invoke + 0x10b, onecore\admin

案例总结：

==========

经与用户确认，在用户修复 wmi 之后可以正常安装软件，经用户同意，此 case 做关闭处理，如后续有其他问题需求，可随时与我联系，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: 2024 年 7 月 24 日 9:53
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-11631-B2M1Q8] %|P2|ICBC|工行用户反馈 V2020-L 版本系统安装软件失败问题% 案例重新分配 CMIT:0001305

许先生，您好:
如刚才电话沟通，针对之前的日志分析，目前判断有一个可能是由于 WMI class 的丢失导致软件的安装失败。接下来请指导用户按照如下方式收集 TSS 日志:

1） 下载 TSS 工具：
https://cduc.cmgos.com/download.php?id=1505&token=rCmPM7GY7750GSSQ9rmMVIpkWCk1kYBj
2） 管理员方式运行 .\TSS.ps1 -Scenario UEX_WMI -procmon
3） 根据提示，复现问题

看到如下的提示，复现问题，复现完问题之后，输入 Y

```
.20240723 17:14:16.763 Calling PSRPreStart
.20240723 17:14:16.934 Calling UEX_COMPreStart
.....................20240723 17:14:18.513 Calling UEX_WMIAdvancedPreStart
.........20240723 17:14:20.955 Calling ProcmonPreStart
..........
.20240723 17:14:21.208 ---------- Start of Repro:  2024-07-23_09:14:21 UTC ----------
Reproduce the issue and press 'Y' key AFTER finishing the repro (with window focus here) [Y]?Y
.20240723 17:14:29.294 ---------- End of Repro:    2024-07-23_09:14:29 UTC ----------
.........20240723 17:14:30.872 Stopping job Procmon.
...20240723 17:14:32.013 Stopping job Netsh.
...20240723 17:14:32.747 Calling UEX_WMIAdvancedPostStop
...20240723 17:14:36.140 Calling UEX_COMPostStop
20240723 17:14:36.171 Stopping job PSR.
..20240723 17:14:36.361 Calling CollectUEX_WMIAdvancedLog
20240723 17:14:36.361 [CollectUEX_WMIAdvancedLog] . calling WMI-Collect.ps1
```

4） 将最后产生的日志发送给我，谢谢。

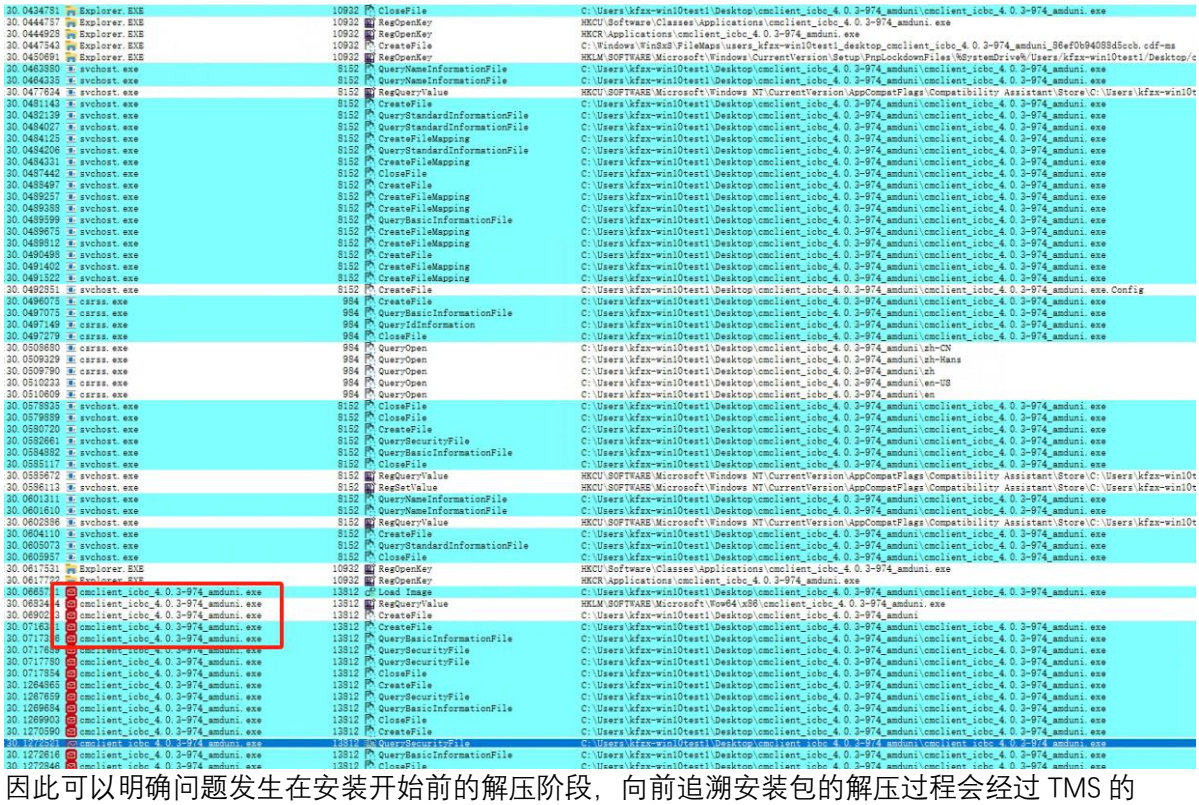
李琦 Li Qi

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

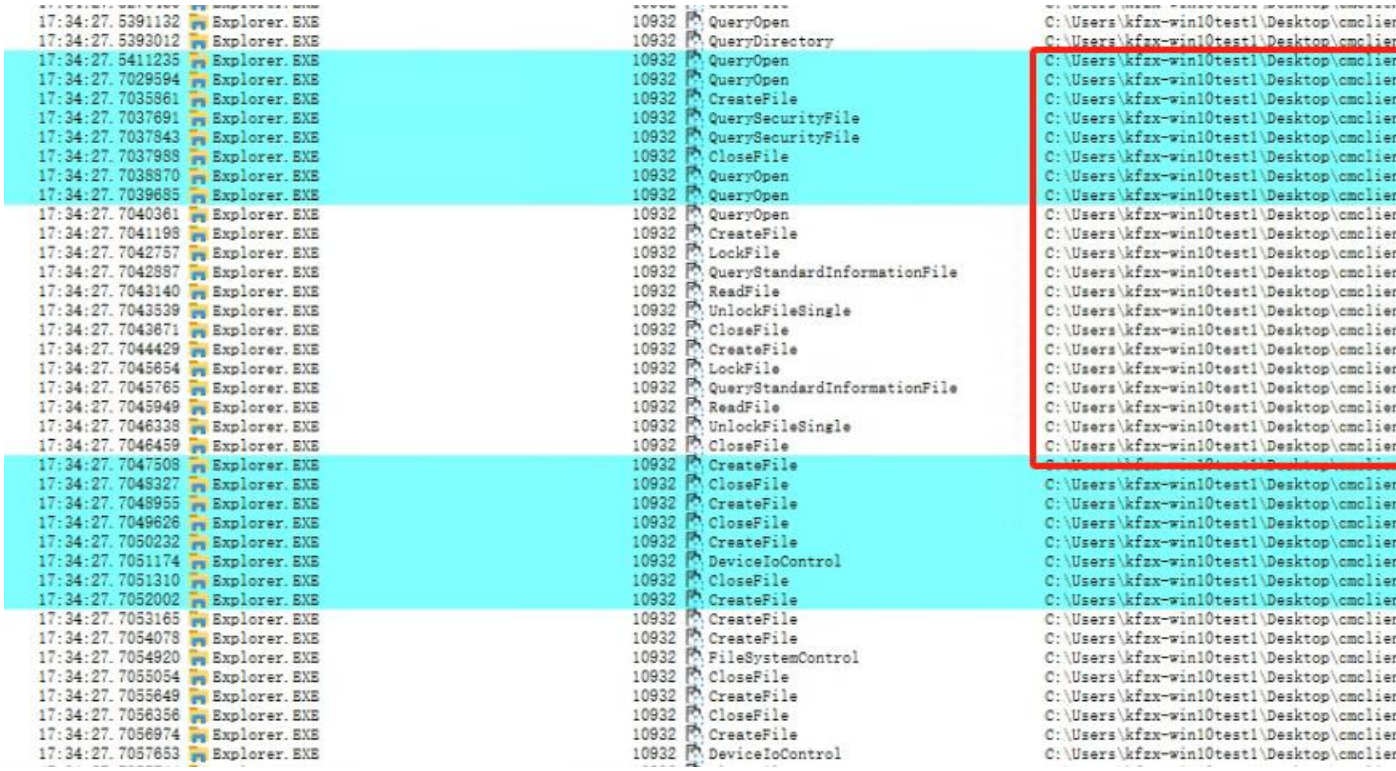
发件人: Li Qi
发送时间: 2024 年 7 月 2 日 15:28
收件人: ICBC 案例通知 <win10sup@sdc.icbc.com.cn>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: [案例号:CAS-11631-B2M1Q8] %|P2|ICBC|工行用户反馈 V2020-L 版本系统安装软件失败问题% 案例重新分配 CMIT:0001305

许先生，您好:

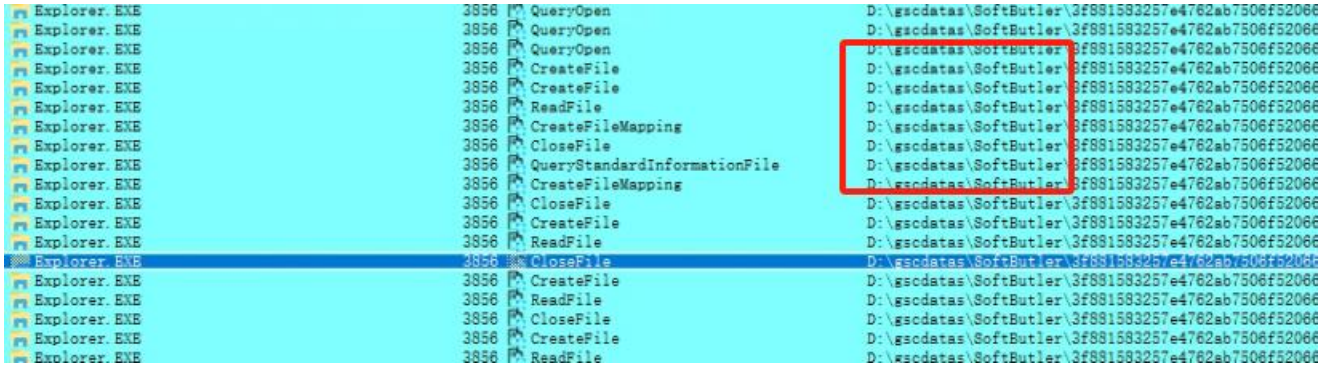
根据您第二份日志中正常与失败的对比日志来看，在解压完成后，会正常进入安装包的安装过程，但失败日志中并没有进入到这个过程



因此可以明确问题发生在安装开始前的解压阶段，向前追溯安装包的解压过程会经过 TMS 的安全审查，审查通过后可以正常安装



而失败的电脑则被移入 TMS 安全审查移入 D:\gscdatas 文件夹过滤掉了，因此不再执行后续安装



因此可以让用户尝试卸载 TMS 完成安装，至于移入 gscdatas 的安全审查标准，请咨询 TMS 厂商处理。

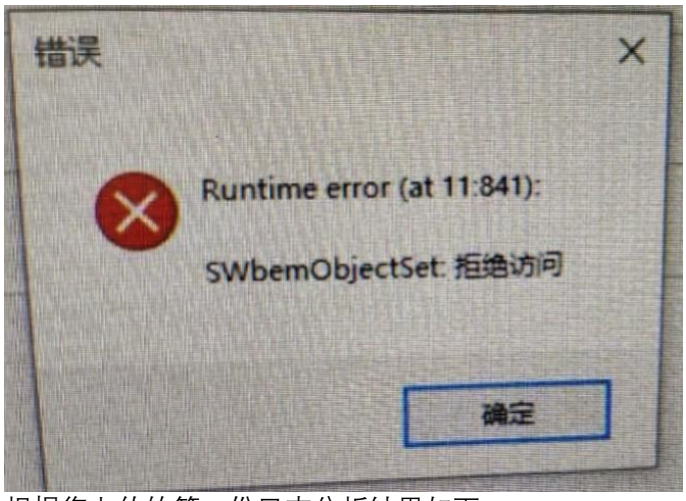
李琦 Li Qi
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话： 4008180055
电子邮箱 Email: liqi@cmgos.com

神州网信
CMIT

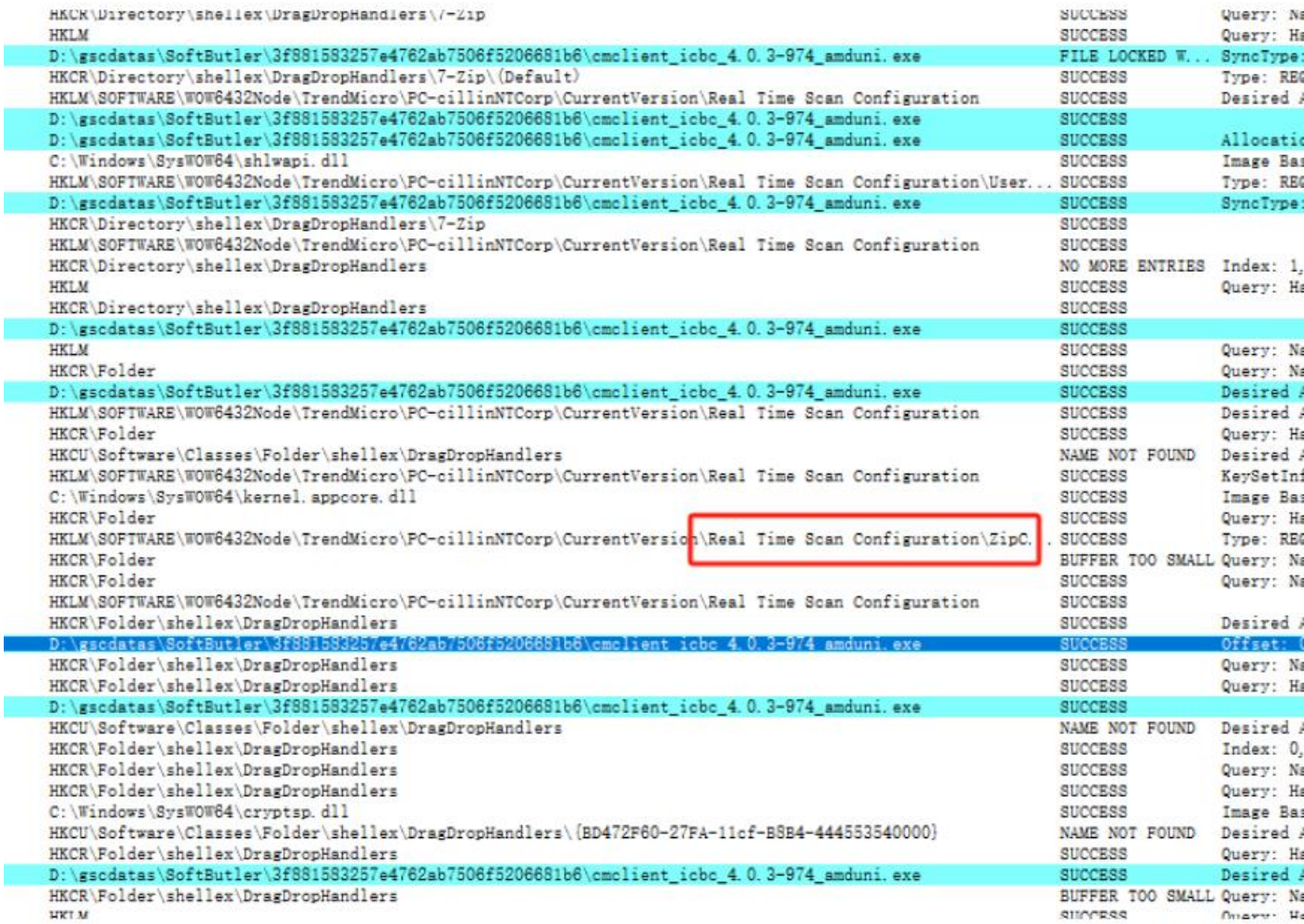
发件人: Li Qi
发送时间: 2024 年 7 月 2 日 10:14
收件人: ICBC 案例通知 <win10sup@sdc.icbc.com.cn>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: [案例号:CAS-11631-B2M1Q8] %|P2|ICBC|工行用户反馈 V2020-L 版本系统安装软件失败问题% 案例重新分配 CMIT:0001305

许先生，您好:

如昨天沟通，当前用户遇到的部分电脑在安装 cmclient 应用过程中发生“拒绝访问”的报错问题。



根据您上传的第一份日志分析结果如下:
首先 procmon 中并没有找到错误弹框的进程，也没有 cmclient 的安装进程。这种情况有可能是在安装过程尚未开始，只是在最开始的安装准备阶段发生的问题。由于我们不清楚应用的安装逻辑，因此从已有的日志记录来看，exe 的执行过程首先会交由 7z 进行解压，而在解压时会交由行业的管控软件进行实时扫描是否合规，而在此过程中出现 access deny 的情况。



HKCR\Directory\shellex\DragDropHandlers\7-Zip	SUCCESS	Query: Na
HKLM	SUCCESS	Query: Ha
D:\gscdatas\SoftButler\3f881583257e4762ab7506f5206681b6\cmclient_icbc_4.0.3-974_amduni.exe	FILE LOCKED W...	SyncType:
HKCR\Directory\shellex\DragDropHandlers\7-Zip\(Default)	SUCCESS	Type: REG
HKLM\SOFTWARE\WOW6432Node\TrendMicro\PC-cillinNTCorp\CurrentVersion\Real Time Scan Configuration	SUCCESS	Desired A
D:\gscdatas\SoftButler\3f881583257e4762ab7506f5206681b6\cmclient_icbc_4.0.3-974_amduni.exe	SUCCESS	
D:\gscdatas\SoftButler\3f881583257e4762ab7506f5206681b6\cmclient_icbc_4.0.3-974_amduni.exe	SUCCESS	Allocatio
C:\Windows\SysWOW64\shlwapi.dll	SUCCESS	Image Bas
HKLM\SOFTWARE\WOW6432Node\TrendMicro\PC-cillinNTCorp\CurrentVersion\Real Time Scan Configuration\User...	SUCCESS	Type: REG
D:\gscdatas\SoftButler\3f881583257e4762ab7506f5206681b6\cmclient_icbc_4.0.3-974_amduni.exe	SUCCESS	SyncType:
HKCR\Directory\shellex\DragDropHandlers\7-Zip	SUCCESS	
HKLM\SOFTWARE\WOW6432Node\TrendMicro\PC-cillinNTCorp\CurrentVersion\Real Time Scan Configuration	SUCCESS	
HKCR\Directory\shellex\DragDropHandlers	NO MORE ENTRIES	Index: 1,
HKLM	SUCCESS	Query: Ha
HKCR\Directory\shellex\DragDropHandlers	SUCCESS	
D:\gscdatas\SoftButler\3f881583257e4762ab7506f5206681b6\cmclient_icbc_4.0.3-974_amduni.exe	SUCCESS	
HKLM	SUCCESS	Query: Na
HKCR\Folder	SUCCESS	Query: Na
D:\gscdatas\SoftButler\3f881583257e4762ab7506f5206681b6\cmclient_icbc_4.0.3-974_amduni.exe	SUCCESS	Desired A
HKLM\SOFTWARE\WOW6432Node\TrendMicro\PC-cillinNTCorp\CurrentVersion\Real Time Scan Configuration	SUCCESS	Desired A
HKCR\Folder	SUCCESS	Query: Ha
HKCU\Software\Classes\Folder\shellex\DragDropHandlers	NAME NOT FOUND	Desired A
HKLM\SOFTWARE\WOW6432Node\TrendMicro\PC-cillinNTCorp\CurrentVersion\Real Time Scan Configuration	SUCCESS	KeySetInf
C:\Windows\SysWOW64\kernel.appcore.dll	SUCCESS	Image Bas
HKCR\Folder	SUCCESS	Query: Ha
HKLM\SOFTWARE\WOW6432Node\TrendMicro\PC-cillinNTCorp\CurrentVersion\Real Time Scan Configuration\ZipC...	SUCCESS	Type: REG
HKCR\Folder	BUFFER TOO SMALL	Query: Na
HKCR\Folder	SUCCESS	Query: Na
HKLM\SOFTWARE\WOW6432Node\TrendMicro\PC-cillinNTCorp\CurrentVersion\Real Time Scan Configuration	SUCCESS	
HKCR\Folder\shellex\DragDropHandlers	SUCCESS	Desired A
D:\gscdatas\SoftButler\3f881583257e4762ab7506f5206681b6\cmclient_icbc_4.0.3-974_amduni.exe	SUCCESS	Offset: 0
HKCR\Folder\shellex\DragDropHandlers	SUCCESS	Query: Na
HKCR\Folder\shellex\DragDropHandlers	SUCCESS	Query: Ha
D:\gscdatas\SoftButler\3f881583257e4762ab7506f5206681b6\cmclient_icbc_4.0.3-974_amduni.exe	SUCCESS	
HKCU\Software\Classes\Folder\shellex\DragDropHandlers	NAME NOT FOUND	Desired A
HKCR\Folder\shellex\DragDropHandlers	SUCCESS	Index: 0,
HKCR\Folder\shellex\DragDropHandlers	SUCCESS	Query: Na
HKCR\Folder\shellex\DragDropHandlers	SUCCESS	Query: Ha
C:\Windows\SysWOW64\cryptsp.dll	SUCCESS	Image Bas
HKCU\Software\Classes\Folder\shellex\DragDropHandlers\{BD472F60-27FA-11cf-B8B4-444553540000}	NAME NOT FOUND	Desired A
HKCR\Folder\shellex\DragDropHandlers	SUCCESS	Query: Ha
D:\gscdatas\SoftButler\3f881583257e4762ab7506f5206681b6\cmclient_icbc_4.0.3-974_amduni.exe	SUCCESS	Desired A
HKCR\Folder\shellex\DragDropHandlers	BUFFER TOO SMALL	Query: Na

由于行内的管控应用执行逻辑复杂，从日志中可以看到 DSP,trend,Asiainfo 均有参与。建议用户先卸载趋势进行排查。

下一步动作：

==========

后续收到用户反馈，卸载趋势后问题依旧。因此收集第二份日志进行排查，为了更好的查看此问题，请收集正常与失败安装的对比日志以查看软件安装的执行逻辑，另外请让用户在问题电脑上执行 CmgeLogCollecter 收集系统日志。以确定具体问题发生点。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: 2024 年 6 月 26 日 16:55
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-11631-B2M1Q8] %|P2|ICBC|工行用户反馈 V2020-L 版本系统安装软件失败问题% 案例重新分配 CMIT:0001305

许先生，您好:

如刚才电话沟通，我谨以此封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:

用户反馈安装软件失败问题，涉及 3-4 台设备，该问题在其他版本操作系统上也有出现，报错为：Swbemobiectset: 拍绝访问。需要协助分析处理。

问题范围:

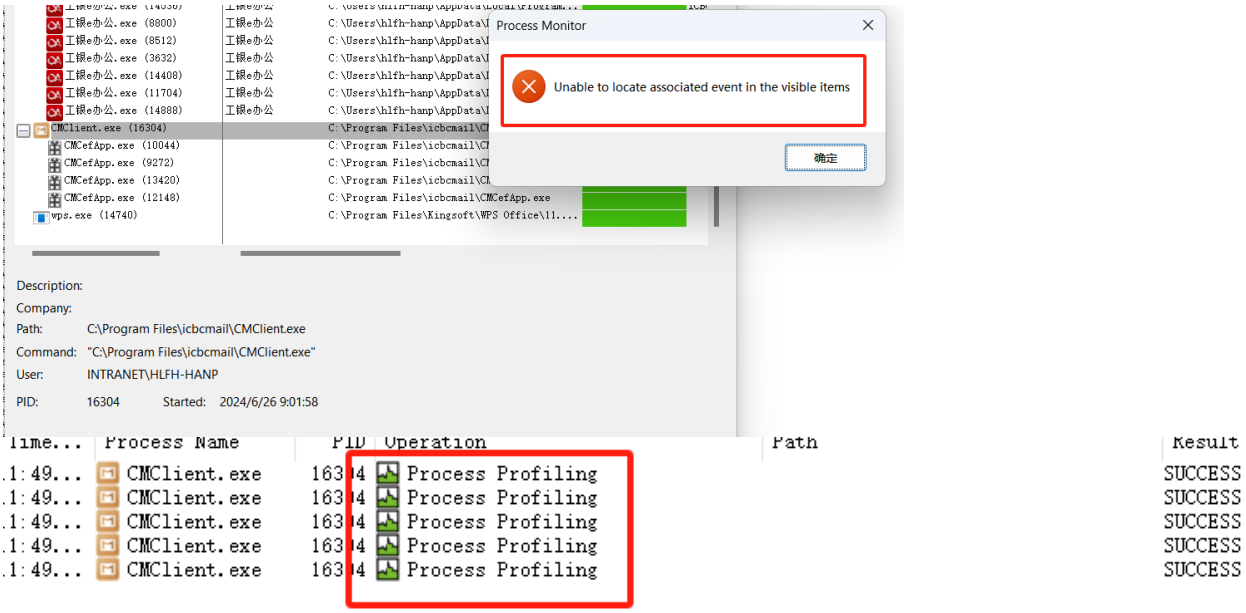
我们将协助您分析处理上述问题，并对定义的问题给予最大的技术支持。

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。

日志分析:

您发送的 procmon 日志无法查看，怀疑与 procmon 版本或用户收取步骤有关。**请指导用户重新收集，最好收集可以安装和安装失败的两份对比日志。**



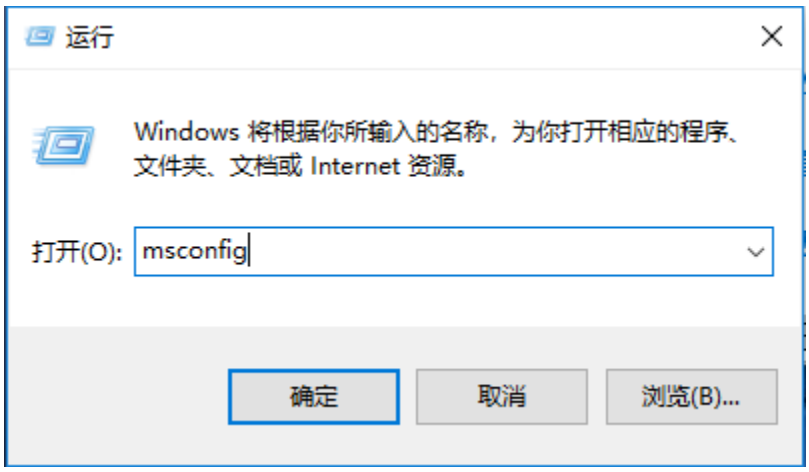
另外为排除第三方软件的干扰，可以指导用户进入 clean boot 再尝试安装看是否正常。以下为进入 clean boot 的方式。

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。

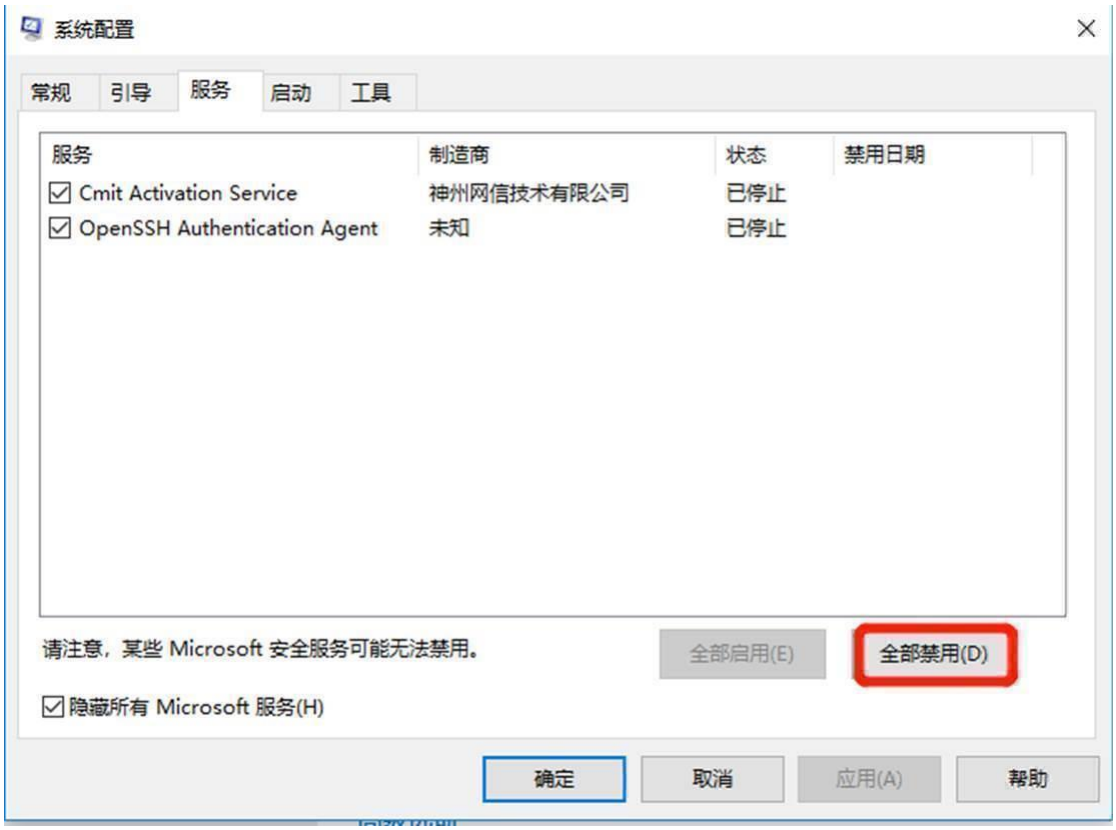
步骤操作：

- 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

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: CRM 管理员 <crmadmin@cmgos.com>
发送时间: 2024 年 6 月 26 日 14:40
收件人: Li Qi <liqi@cmgos.com>
主题: [案例号:CAS-11631-B2M1Q8] %|P2|ICBC|工行用户反馈 V2020-L 版本系统安装软件失败问题% 案例重新分配 CMIT:0001305

Hi 李琦

一个案例已被重新分配给您，请及时处理。

案例号码： CAS-11631-B2M1Q8
案例等级： P2
案例描述： 接到工行接口人许翔来电，反馈 V2020-L 版本系统安装软件失败问题，涉及 3-4 台设备，用户未提供具体软件名称及报错信息，称已收集日志，需要协助分析处理。
申请开启 P2 案例。

用户信息如下
单位：中国工商银行股份有限公司
联系人：许翔
电话：17606669571
邮箱：win10sup@sdc.icbc.com.cn
ACCESSID：25240869
创建人： 吴闫杰
创建时间： 2024/6/26 14:30