

杨女士，您好

很高兴与您沟通，根据目前的案例情况，我将暂时归档此问题。**案例归档后您会收到调查问卷的邮件，希望可以对我们的服务进行评价。**

案例总结：

案例描述：

反馈 Windows 7 版本系统调用外设（扫描仪）失败问题，涉及 1-2 台电脑，需要协助分析处理。

案例进展：

读取 java 虚拟机运行环境时未正常读取 java 虚拟机的多个模块。

由于从操作系统层面只能看到进程信息，对于未能正常读取 java 模块的过程无法查看到更为细节的内容。

建议确认 java 虚拟机运行环境，再测试卸载 DSP 应用，排除 DSP 应用的影响。

贾伟 Jia Wei
神州网信技术有限公司
服务支持电话： 400-818-0055
电子邮箱： jiawei@cmgos.com

C&M Information Technologies Co., Ltd.
11F, Block C North Building, Raycom InfoTech Park, Beijing
mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人: Jia Wei

发送时间: 2024 年 6 月 13 日 13:41

收件人: 2870654105@qq.com

抄送: ICBC 案例通知 <win10sup@sdicbc.com.cn>; ICBC_Notification
<ICBC_Notification@cmgos.com>

主题: 回复: [案例号: CAS-11431-B7W6M8] % |P2|ICBC|工行用户反馈 V2020-L 版本系统调用外设失败问题 % 初次响应 CMIT:0001870

杨女士 您好:

来信是跟踪当前案例的进展

如果您有疑问或反馈, 可以回复此邮件。

贾伟 Jia Wei
神州网信技术有限公司
服务支持电话: 400-818-0055
电子邮箱: jiawei@cmgos.com

C&M Information Technologies Co., Ltd.
11F, Block C North Building, Raycom InfoTech Park, Beijing
mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人: Wei Liang <weiliang@cmgos.com>

发送时间: 2024 年 6 月 7 日 17:22

收件人: Jia Wei <jiawei@cmgos.com>; 2870654105@qq.com

抄送: ICBC 案例通知 <win10sup@sdicbc.com.cn>; ICBC_Notification
<ICBC_Notification@cmgos.com>

主题: 回复: [案例号: CAS-11431-B7W6M8] % |P2|ICBC|工行用户反馈 V2020-L 版本系统调用外设失败问题 % 初次响应 CMIT:0001870

杨女士 您好:

根据您提供的信息, 在调用外设时, 会拉起 eapbrowser 模块, 此模块需要 java 虚拟机运行。

对比您提供的出现调用外设异常和调用正常的 procmon 日志, 可以看到:

异常日志在读取 java 虚拟机运行环境时未正常读取 java 虚拟机的多个模块, 期间还有 DSP 应用的参与。

PID	Operation	Path
10188	ReadFile	D:\icbc\CsspDeviceServer\lib_diy\windows\jdk1.8win32\jre\bin\server\jvm.dll
10188	ReadFile	D:\icbc\CsspDeviceServer\lib_diy\windows\jdk1.8win32\jre\bin\server\jvm.dll
10188	ReadFile	D:\icbc\CsspDeviceServer\lib_diy\windows\jdk1.8win32\jre\bin\server\jvm.dll
10188	ReadFile	D:\icbc\CsspDeviceServer\lib_diy\windows\jdk1.8win32\jre\bin\server\jvm.dll
10188	ReadFile	D:\icbc\CsspDeviceServer\lib_diy\windows\jdk1.8win32\jre\bin\server\jvm.dll
10188	ReadFile	D:\icbc\CsspDeviceServer\lib_diy\windows\jdk1.8win32\jre\bin\server\jvm.dll
10188	ReadFile	D:\icbc\CsspDeviceServer\lib_diy\windows\jdk1.8win32\jre\bin\server\jvm.dll
10188	CloseFile	C:\Users\fjqz-huangbb\AppData\Local\Temp\hsperfdata_fjqz-huangbb\10188
10188	Thread Exit	
10188	Thread Exit	
10188	Thread Exit	
10188	ReadFile	D:\icbc\CsspDeviceServer\lib_diy\windows\jdk1.8win32\jre\bin\server\jvm.dll
10188	ReadFile	C:\Program Files\DSPClient\CEMS\EDSM\MedWaterMarkM.dll
10188	ReadFile	C:\Program Files\DSPClient\CEMS\EDSM\MedWaterMarkM.dll
10188	ReadFile	C:\Program Files\DSPClient\CEMS\EDSM\MedWaterMarkM.dll
10188	ReadFile	C:\Program Files\DSPClient\CEMS\EDSM\MedWaterMarkM.dll
10188	ReadFile	C:\Windows\System32\wininet.dll
10188	ReadFile	C:\Windows\System32\wininet.dll
10188	ReadFile	C:\Windows\System32\iertutil.dll
10188	ReadFile	C:\Program Files\DSPClient\CEMS\EDSM\MedAdapter.dll
10188	ReadFile	C:\Program Files\DSPClient\CEMS\EDSM\vEdsmOfficeExt.dll
10188	ReadFile	C:\Program Files\DSPClient\CEMS\EDSM\vEdsmOfficeExt.dll
10188	ReadFile	C:\Program Files\DSPClient\CEMS\EDSM\MedEoDataCtrlEx.dll
10188	ReadFile	C:\Program Files\DSPClient\CEMS\EDSM\MedEoDataCtrlEx.dll
10188	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Compatibility32
10188	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Compatibility32\pyDeviceService
10188	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Compatibility32
10188	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\IME Compatibility
10188	ReadFile	C:\Program Files\DSPClient\CEMS\EDSM\PrintWatermark.dll
10188	ReadFile	C:\Program Files\DSPClient\CEMS\EDSM\PrintWatermark.dll
10188	ReadFile	C:\Program Files\DSPClient\CEMS\EDSM\PrintWatermark.dll
10188	ReadFile	C:\Program Files\DSPClient\CEMS\EDSM\PrintWatermark.dll
10188	ReadFile	C:\Program Files\DSPClient\CEMS\EDSM\medscreenm.dll
10188	ReadFile	C:\Program Files\DSPClient\CEMS\EDSM\medscreenm.dll
10188	ReadFile	C:\Program Files\DSPClient\CEMS\EDSM\medscreenm.dll
10188	ReadFile	C:\Program Files\DSPClient\CEMS\EDSM\EnsecCore.dll
10188	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize
10188	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
10188	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize
10188	Thread Exit	
10188	QueryNameInform...	D:\icbc\CsspDeviceServer\pyDeviceService.exe
10188	QueryNameInform...	D:\icbc\CsspDeviceServer\lib_diy\windows\jdk1.8win32\jre\bin\server\jvm.dll

而正常日志显示访问了 java 虚拟机的模块，后续继续访问了 eapbrowser.jar 模块以及 eap 的页面。

[illegible]


```
1784 CloseFile D:\ICBC\CsspDeviceServer
1784 CreateFile D:\ICBC\CsspDeviceServer\lib_diy
1784 QueryDirectory D:\ICBC\CsspDeviceServer\lib_diy\windows
1784 QueryNameInformationFile D:\ICBC\CsspDeviceServer\lib_diy
1784 QueryNameInform... D:\ICBC\CsspDeviceServer\lib_diy
1784 QueryNameInform... D:\ICBC\CsspDeviceServer\lib_diy
1784 CloseFile D:\ICBC\CsspDeviceServer\lib_diy
1784 CreateFile D:\ICBC\CsspDeviceServer\lib_diy\windows
1784 QueryDirectory D:\ICBC\CsspDeviceServer\lib_diy\windows\EapBrowser.jar
1784 QueryNameInform... D:\ICBC\CsspDeviceServer\lib_diy\windows
1784 QueryNameInform... D:\ICBC\CsspDeviceServer\lib_diy\windows
1784 QueryNameInform... D:\ICBC\CsspDeviceServer\lib_diy\windows
1784 CloseFile D:\ICBC\CsspDeviceServer\lib_diy\windows
1784 QueryOpen D:\ICBC\CsspDeviceServer\lib_diy\windows\EapBrowser.jar
1784 QueryOpen D:\ICBC\CsspDeviceServer\lib_diy\windows\EapBrowser.jar
1784 ReadFile D:\ICBC\CsspDeviceServer\lib_diy\windows\jdk1.8win32\jre\lib\rt.jar
1784 ReadFile D:\ICBC\CsspDeviceServer\lib_diy\windows\jdk1.8win32\jre\lib\rt.jar
1784 ReadFile D:\ICBC\CsspDeviceServer\lib_diy\windows\jdk1.8win32\jre\lib\rt.jar
1784 ReadFile D:\ICBC\CsspDeviceServer\lib_diy\windows\jdk1.8win32\jre\lib\rt.jar
1784 ReadFile D:\ICBC\CsspDeviceServer\lib_diy\windows\jdk1.8win32\jre\lib\rt.jar
1784 ReadFile D:\ICBC\CsspDeviceServer\lib_diy\windows\jdk1.8win32\jre\lib\rt.jar
1784 ReadFile D:\ICBC\CsspDeviceServer\lib_diy\windows\jdk1.8win32\jre\lib\rt.jar
1784 ReadFile D:\ICBC\CsspDeviceServer\lib_diy\windows\jdk1.8win32\jre\lib\rt.jar
1784 ReadFile D:\ICBC\CsspDeviceServer\lib_diy\windows\jdk1.8win32\jre\lib\rt.jar
1784 ReadFile D:\ICBC\CsspDeviceServer\lib_diy\windows\jdk1.8win32\jre\lib\rt.jar
1784 QueryOpen D:\ICBC\CsspDeviceServer\lib_diy\windows\EapBrowser.jar
1784 ReadFile D:\ICBC\CsspDeviceServer\lib_diy\windows\jdk1.8win32\jre\lib\rt.jar
1784 ReadFile D:\ICBC\CsspDeviceServer\lib_diy\windows\jdk1.8win32\jre\lib\rt.jar

1784 RegOpenKey HKCU\Software\Classes\CLSID\{00020420-0000-0000-0000-000000000040}\TreatAs NAME ?
1784 RegOpenKey HKCR\CLSID\{00020420-0000-0000-0000-000000000040}\TreatAs NAME ?
1784 RegCloseKey HKCR\CLSID\{00020420-0000-0000-0000-000000000040} SUCCESS
1784 ReadFile D:\ICBC\CsspDeviceServer\lib_diy\windows\swt3.0.2.jar SUCCESS
1784 ReadFile D:\ICBC\CsspDeviceServer\lib_diy\windows\swt3.0.2.jar SUCCESS
1784 ReadFile D:\ICBC\CsspDeviceServer\lib_diy\windows\swt3.0.2.jar SUCCESS
1784 ReadFile D:\ICBC\CsspDeviceServer\lib_diy\windows\swt3.0.2.jar SUCCESS
1784 ReadFile D:\ICBC\CsspDeviceServer\lib_diy\windows\swt3.0.2.jar SUCCESS
1784 ReadFile D:\ICBC\CsspDeviceServer\lib_diy\windows\swt3.0.2.jar SUCCESS
1784 ReadFile D:\ICBC\CsspDeviceServer\lib_diy\windows\swt3.0.2.jar SUCCESS
1784 ReadFile D:\ICBC\CsspDeviceServer\lib_diy\windows\swt3.0.2.jar SUCCESS
1784 ReadFile D:\ICBC\CsspDeviceServer\lib_diy\windows\swt3.0.2.jar SUCCESS
1784 ReadFile D:\ICBC\CsspDeviceServer\lib_diy\windows\swt3.0.2.jar SUCCESS
1784 ReadOpenKey HKLM\Software\Microsoft\OleAut NAME ?
1784 ReadFile D:\ICBC\CsspDeviceServer\lib_diy\windows\json.jar SUCCESS
1784 ReadFile D:\ICBC\CsspDeviceServer\lib_diy\windows\json.jar SUCCESS
1784 ReadFile D:\ICBC\CsspDeviceServer\lib_diy\windows\json.jar SUCCESS
1784 CreateFile C:\Program Files\ICBC\EapClient\Web\ctbui\CSSP\eap-scan.html SUCCESS
1784 QueryInformati... C:\Program Files\ICBC\EapClient\Web\ctbui\CSSP\eap-scan.html BUFFER
1784 QueryAllInforma... C:\Program Files\ICBC\EapClient\Web\ctbui\CSSP\eap-scan.html BUFFER
1784 CloseFile C:\Program Files\ICBC\EapClient\Web\ctbui\CSSP\eap-scan.html SUCCESS
1784 CreateFile C:\Program Files\ICBC\EapClient\data SUCCESS
1784 QueryDirectory C:\Program Files\ICBC\EapClient\data SUCCESS
```

测试建议：

- 1) 请您先在问题设备上确认 CsspDeviceServer 自带的 java 虚拟机运行环境是否正常，请您在问题设备上测试其 java 虚拟机运行环境。
是否可以在问题设备上直接测试自带的 java 虚拟机运行 eapbrowser.jar 模块。
java 虚拟机运行环境路径：D:\ICBC\CsspDeviceServer\lib_diy\windows\jdk1.8win32\jre\
- 2) 确认其他的 Win7 系统安装了 DSP 应用的设备是否可以正常调用外设，或者测试卸载 DSP 应用，排除 DSP 应用的影响。

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: Jia Wei <jiawei@cmgos.com>

发送时间: 2024 年 5 月 30 日 17:55

收件人: 2870654105@qq.com

抄送: ICBC 案例通知 <win10sup@sdicbc.com.cn>; ICBC_Notification
<ICBC_Notification@cmgos.com>

主题: 回复: [案例号: CAS-11431-B7W6M8] % |P2|ICBC|工行用户反馈 V2020-L 版本系统
调用外设失败问题 % 初次响应 CMIT:0001870

杨女士，您好

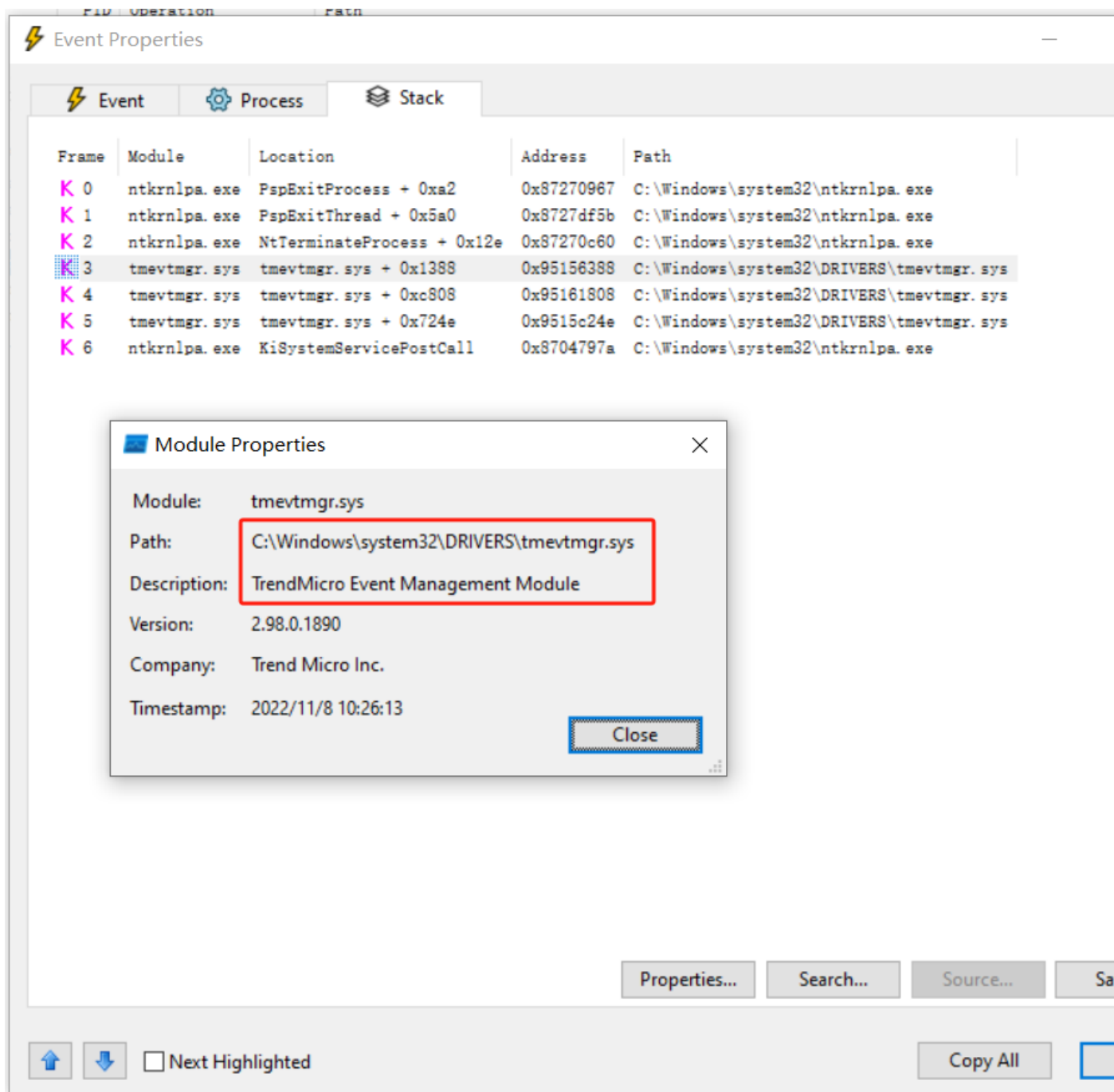
很高兴与您电话沟通。

案例分析：

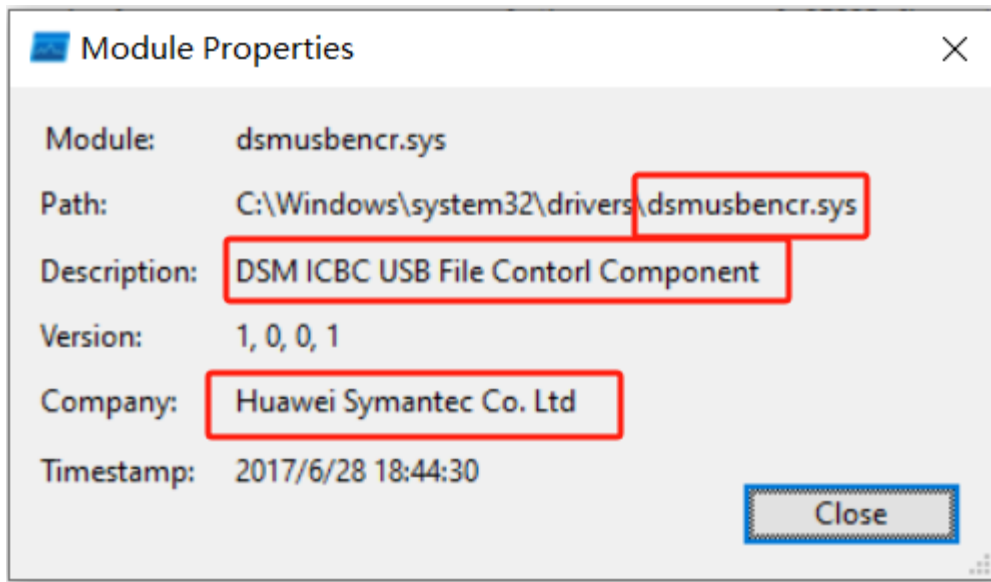
如之前沟通的结果，目前看到问题过程中有大量 pyDeviceService.exe 进程被创建出来，其中
PID 为 13512 的进程在日志收集过程中终止了

Process	Description	Image Path
sguardc.exe (3928)		C:\Windows\System32\Pclient\app\sguardc.exe
sccltui.exe (6316)		C:\Windows\System32\Pclient\app\sccltui.exe
CsspDeviceServer.exe (8344)		D:\icbc\CsspDeviceServer\CsspDeviceServer.exe
cmd.exe (13124)		C:\Windows\system32\cmd.exe
pyDeviceService.exe (1812)		D:\icbc\CsspDeviceServer\pyDeviceService.exe
pyDeviceService.exe (8768)		D:\icbc\CsspDeviceServer\pyDeviceService.exe
pyDeviceService.exe (11112)		D:\icbc\CsspDeviceServer\pyDeviceService.exe
pyDeviceService.exe (9536)		D:\icbc\CsspDeviceServer\pyDeviceService.exe
pyDeviceService.exe (14668)		D:\icbc\CsspDeviceServer\pyDeviceService.exe
pyDeviceService.exe (11924)		D:\icbc\CsspDeviceServer\pyDeviceService.exe
pyDeviceService.exe (12436)		D:\icbc\CsspDeviceServer\pyDeviceService.exe
pyDeviceService.exe (6372)		D:\icbc\CsspDeviceServer\pyDeviceService.exe
pyDeviceService.exe (14324)		D:\icbc\CsspDeviceServer\pyDeviceService.exe
pyDeviceService.exe (8584)		D:\icbc\CsspDeviceServer\pyDeviceService.exe
pyDeviceService.exe (13392)		D:\icbc\CsspDeviceServer\pyDeviceService.exe
pyDeviceService.exe (6292)		D:\icbc\CsspDeviceServer\pyDeviceService.exe
pyDeviceService.exe (9376)		D:\icbc\CsspDeviceServer\pyDeviceService.exe
pyDeviceService.exe (13512)		D:\icbc\CsspDeviceServer\pyDeviceService.exe
pyDeviceService.exe (13544)		D:\icbc\CsspDeviceServer\pyDeviceService.exe
pyDeviceService.exe (14860)		D:\icbc\CsspDeviceServer\pyDeviceService.exe
pyDeviceService.exe (13852)		D:\icbc\CsspDeviceServer\pyDeviceService.exe
pyDeviceService.exe (13352)		D:\icbc\CsspDeviceServer\pyDeviceService.exe
pyDeviceService.exe (1612)		D:\icbc\CsspDeviceServer\pyDeviceService.exe
pyDeviceService.exe (2028)		D:\icbc\CsspDeviceServer\pyDeviceService.exe
pyDeviceService.exe (7868)		D:\icbc\CsspDeviceServer\pyDeviceService.exe
pyDeviceService.exe (15596)		D:\icbc\CsspDeviceServer\pyDeviceService.exe
pyDeviceService.exe (8540)		D:\icbc\CsspDeviceServer\pyDeviceService.exe
pyDeviceService.exe (9744)		D:\icbc\CsspDeviceServer\pyDeviceService.exe
pyDeviceService.exe (10236)		D:\icbc\CsspDeviceServer\pyDeviceService.exe
pyDeviceService.exe (14748)		D:\icbc\CsspDeviceServer\pyDeviceService.exe
pyDeviceService.exe (9072)		D:\icbc\CsspDeviceServer\pyDeviceService.exe
pyDeviceService.exe (15852)		D:\icbc\CsspDeviceServer\pyDeviceService.exe
pyDeviceService.exe (16332)		D:\icbc\CsspDeviceServer\pyDeviceService.exe
pyDeviceService.exe (10708)		D:\icbc\CsspDeviceServer\pyDeviceService.exe
pyDeviceService.exe (11128)		D:\icbc\CsspDeviceServer\pyDeviceService.exe
pyDeviceService.exe (12924)		D:\icbc\CsspDeviceServer\pyDeviceService.exe
pyDeviceService.exe (7052)		D:\icbc\CsspDeviceServer\pyDeviceService.exe

进程退出过程中有 **tmevtmgr.sys** filter driver 文件介入，此文件应该是 TrendMicro 开发，趋势反病毒软件相关组件。



此外还有 **dsmusbencr.sys** 文件也在过程中大量出现。对应的是华为 DSM，时间戳看也很久没有更新过了。



建议操作：

目前从系统层面只能从 Procmon 日志中检索可疑的三方组件，并采用排除法卸载对应的应用。

建议逐一卸载，确认问题是否解决

- 趋势反病毒软件
- DSM

日志收集：

同时可以按照附件《Full dump 配置方法》配置 Full dump，再以管理员身份运行 cmd，依次运行如下命令配置注册表键值

```
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting\LocalDumps" /v DumpCount /t REG_DWORD /d 10 /f
```

```
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting\LocalDumps" /v DumpFolder /t REG_EXPAND_SZ /d %LOCALAPPDATA%\CrashDumps /f
```

```
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting\LocalDumps" /v DumpType /t REG_DWORD /d 2 /f
```

配置完毕之后，复现问题现象，如果过程中出现进程崩溃“1000”的事件日志，就会在%LOCALAPPDATA%\CrashDumps 目录下生成 dmp 日志，将日志反馈。

贾伟 Jia Wei
神州网信技术有限公司
服务支持电话： 400-818-0055
电子邮箱： jiawei@cmgos.com

C&M Information Technologies Co., Ltd.
11F, Block C North Building, Raycom InfoTech Park, Beijing
mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人: Jia Wei
发送时间: 2024 年 5 月 24 日 16:32
收件人: '2870654105@qq.com' <2870654105@qq.com>
抄送: ICBC 案例通知 <win10sup@sdicbc.com.cn>; ICBC_Notification
<ICBC_Notification@cmgos.com>
主题: 回复: [案例号: CAS-11431-B7W6M8] % |P2|ICBC|工行用户反馈 V2020-L 版本系统
调用外设失败问题 % 初次响应 CMIT:0001870

杨女士，您好

很高兴与您电话沟通。基于目前在其他 Windows 7 机器可以正常调用扫描仪外设，您可以参考**建议操作**进行问题排查：

问题定义:

反馈 Windows 7 版本系统调用外设（扫描仪）失败问题，涉及 1-2 台电脑，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。

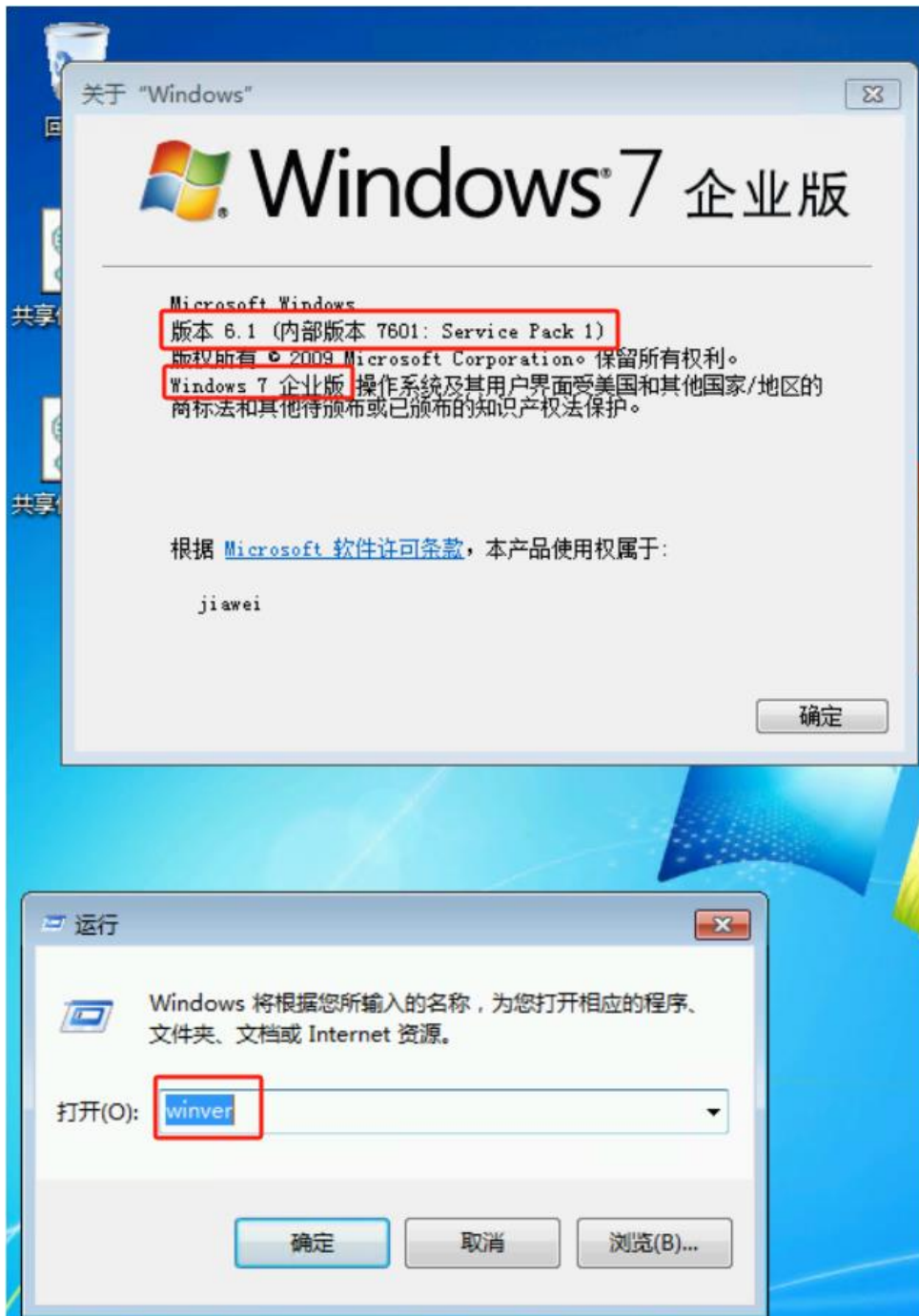
如果能及时解决问题，或问题属于产品设计的行为，或问题涉及到三方，我们将考虑关闭案例。如果存在多个问题，则我们考虑拆分案例进行分析。

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。

- 1) 确认问题计算机上的 Win 7 版本和正常调用外设设备的计算机 Win 7 版本是否一致。如果不一致则建议使用同样的操作系统版本

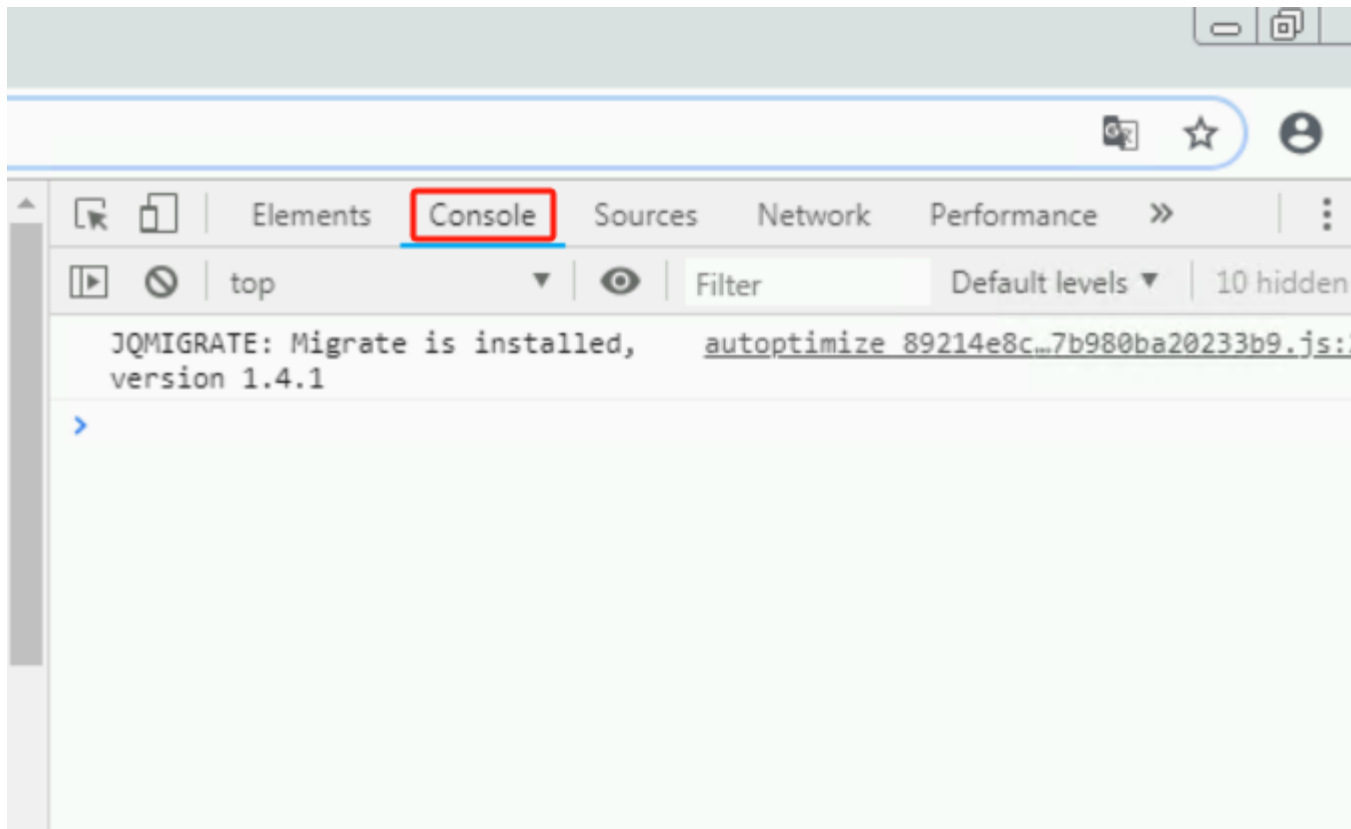
例如是否都是同一版本（企业版？专业版）32 位或 64 位，以及目前的内部版本（Service Pack 版本）

同时按下 Windows+R，运行 winver 可以查看



- 2) 查看安装的 Chrome 浏览器版本是否一致。如不一致建议在问题机器上，安装可以正常加载外设设备系统上的 Chrome 版本；

- 3) 如果上述均保持一致，可以进入 Chrome F12，在 Console 中对比查看两台计算机点击调用外设设备按钮之后，所反馈的报错信息。



贾伟 Jia Wei
神州网信技术有限公司
服务支持电话： 400-818-0055
电子邮箱： jiawei@cmgos.com

C&M Information Technologies Co., Ltd.
11F, Block C North Building, Raycom InfoTech Park, Beijing
mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人: Jia Wei <jiawei@cmgos.com>
发送时间: 2024 年 5 月 24 日 15:33
收件人: ICBC 案例通知 <win10sup@sdicbc.com.cn>
抄送: Jia Wei <jiawei@cmgos.com>
主题: [案例号: CAS-11431-B7W6M8] % |P2|ICBC|工行用户反馈 V2020-L 版本系统调用外设失败问题 % 初次响应 CMIT:0001870

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 贾伟 。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-11431-B7W6M8 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”。