唐女士，您好：

如昨天电话沟通，当前此问题判断为 23 年 7B 累积更新导致的功能性 bug 导致，经您的确认，您已知悉此情况，该问题将做归档处理，以下为案例总结：

Case No：CAS-10387-B9Z9T1

问题描述：

==========

反馈 V2020-L 版本系统安装 KB5030214 补丁后打印异常，报错代码为：0x80004005。需要协助分析处理

问题分析：

==========

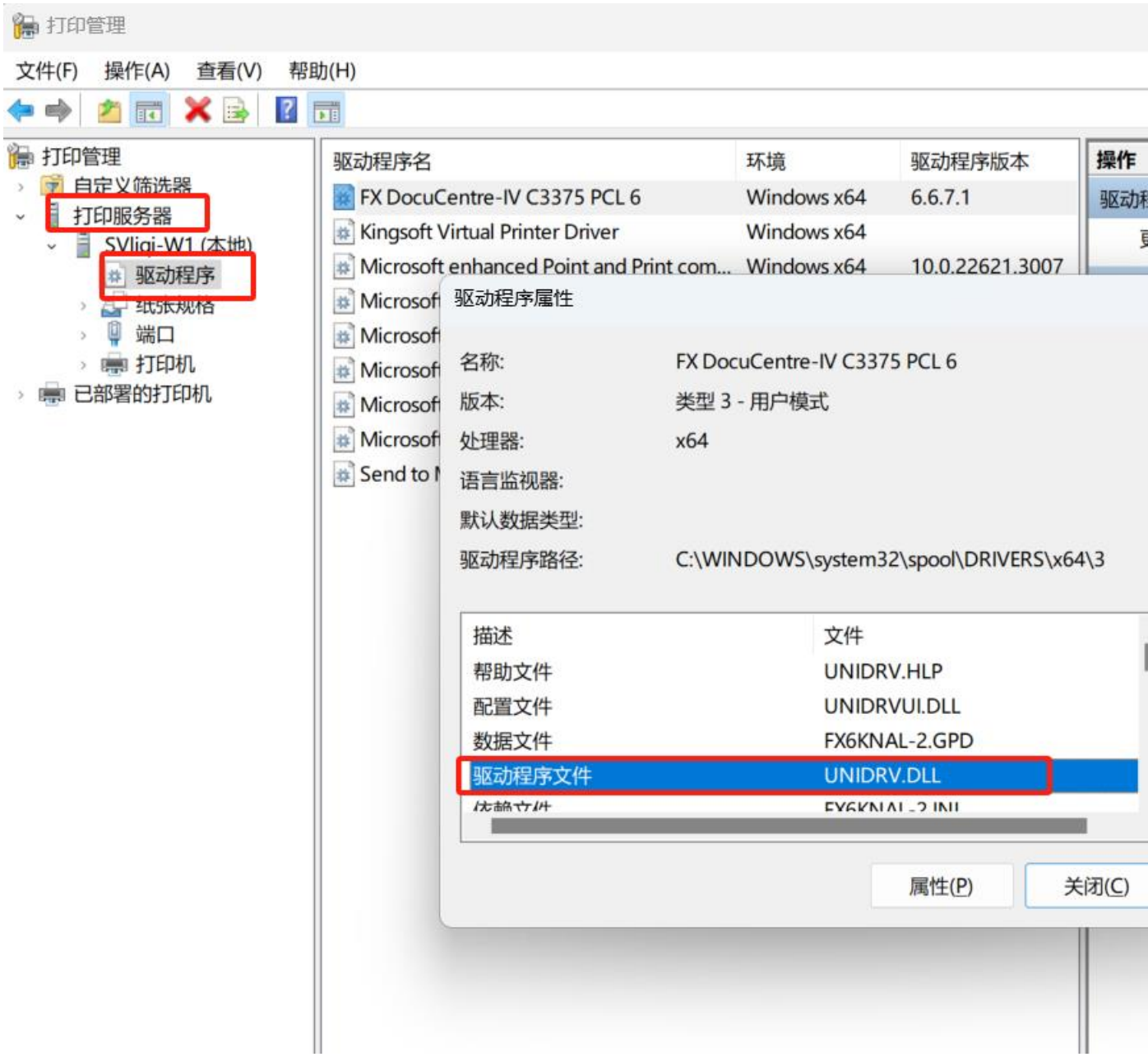
经日志分析与代码查询，发现自 23 年 7B 的累积更新安装之后，当使用 unidrv 关联打印驱动做图片预览时，处理逻辑进行了优化，这一优化导致 BindPrinter 绘图预览时检测到 CreateDC 失败进而导致异常，这是发生当前问题的根本原因，安装后续补丁也会优化该处理逻辑。该问题属于累积更新补丁带来的功能性 bug，受影响范围包括：基于 1809 版本的 V 2020-L 和基于 21H2 版本的 V2022-L。

针对此问题，目前可供您参考的处理方法有两种：

1，不使用照片应用进行图片打印。

2，联系打印机厂商更新打印机驱动或更换打印机，不使用 unidrv.dll 作为打印驱动程序文件的打印机进行照片应用内的打印。作为参考，您可以使用如下方法确认当前打印机所使用的驱动程序文件。

具体方法为：按 Win+R，在输入框中输入“printmanagement.msc”，点击“打印服务器”-“本地”-“驱动程序”，右键选择右侧列表中打印机的“属性”，查看驱动程序文件，是否为 UNIDRV.DLL



案例总结：

==========

经用户确认，用户已知悉上述情况。经用户同意，该 case 将做归档处理，如有其他问题，可随时联系我们，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 1 月 17 日 17:24
收件人: '张' <1257503651@qq.com>; '唐晨明' <tangchenming_cz@js.icbc.com.cn>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>; ICBC 案例通知 <win10sup@sdc.icbc.com.cn>
主题: 回复: 回复: [案例号: CAS-10387-B9Z9T1] % |P2|ICBC|工行反馈在 V2020-L 版本安装 KB5030214 补丁后打印异常 % 初次响应 CMIT:0001601

Hi, All:
当前问题的分析结果如下，请参考:
问题时刻异常点发生在 CalculatePrintableArea 相关处理上，而其处理过程中 getdevcaps 部分有被 schk_x64 hook。另外好坏场景用的驱动也有所不同，你的异常场景中 Pantum CP2257DN HBP 使用的是 UNIDRV 驱动执行绘图关联操作，而 RICOH MP 3555 PCL 6_2 用的是并非 UNIDRV.dll，简单来讲就是好坏场景在这部分处理逻辑不同

PrintDialog TTD:
DbgID ThreadID User Kernel Position Approx. System Time COM-Initialized
5 25d8 (0n9688) 0s 0s 00431DF3:0072 Thursday, January 11, 2024 2:56:56.391 AM ApartmentType_MTA

```
# Call Site
0 PrintDialog!wil::details::ReportFailure+0x0
1 PrintDialog!wil::details::ReportFailure_Hr+0x44
2 PrintDialog!wil::details::in1diag3::_Throw_Hr+0x25
3 PrintDialog!wil::details::in1diag3::Throw_IfFailed+0x1a9
4 PrintDialog!<lambda_361a11138f2d753fa3792d41da618c5f>::operator()+0x384
5 PrintDialog!Concurrency::details::_SelectorTaskGenerator<Concurrency::details::_TypeSelectorNoAsync,Windows::Foundation::HResult>::_GenerateTask_0::__l2::<lambda_66bda433bab03bd3f5b88a24ea8a1f1a>::operator()+0xc
6 PrintDialog!std::_Callable_obj<<lambda_66bda433bab03bd3f5b88a24ea8a1f1a>,0>::_ApplyX+0xc
7 PrintDialog!std::_Func_impl<std::_Callable_obj<<lambda_66bda433bab03bd3f5b88a24ea8a1f1a>,0>,std::allocator<std::_Func_class<Windows::Foundation::HResult,std::_Nil,std::_Nil,std::_Nil,std::_Nil,std::_Nil,std::_Nil,std::_Nil> >,Windows::Foundation::HResult,std::_Nil,std::_Nil,std::_Nil,std::_Nil,std::_Nil,std::_Nil,std::_Nil>::_Do_call+0x12
```

8
PrintDialog!std::_Func_class<Windows::Foundation::HResult,std::_Nil,std::_Nil,std::_Nil,std::_Nil,std::_Nil,std::_Nil,std::_Nil>::operator()+0x19
9
PrintDialog!Concurrency::task<Windows::Foundation::HResult>::_InitialTaskHandle<Windows::Foundation::HResult,<lambda_66bda433bab03bd3f5b88a24ea8a1f1a>,Concurrency::details::_TypeSelectorNoAsync>::_Init+0x104
a
PrintDialog!Concurrency::task<Windows::Foundation::HResult>::_InitialTaskHandle<Windows::Foundation::HResult,<lambda_66bda433bab03bd3f5b88a24ea8a1f1a>,Concurrency::details::_TypeSelectorNoAsync>::_Perform+0x8
b
PrintDialog!Concurrency::details::_PPLTaskHandle<Windows::Foundation::HResult,Concurrency::task<Windows::Foundation::HResult>::_InitialTaskHandle<Windows::Foundation::HResult,<lambda_66bda433bab03bd3f5b88a24ea8a1f1a>,Concurrency::details::_TypeSelectorNoAsync>,pplx::details::_UnrealizedChore>::operator()+0x70
c PrintDialog!Custom::_RunChoreBridge+0x21
d
PrintDialog!Windows::System::Threading::WorkItemHandler::[Windows::System::Threading::WorkItemHandler::__abi_IDelegate]::__abi_Windows_System_Threading_WorkItemHandler___abi_IDelegate____abi_Invoke+0x34
e
threadpoolwinrt!Windows::System::Threading::CThreadPoolWorkItem::CommonWorkCallback+0xaa
f threadpoolwinrt!Windows::System::Threading::CThreadPoolWorkItem::BatchedCallback+0xac
10 ntdll!TppWorkpExecuteCallback+0x130
11 ntdll!TppWorkerThread+0x644
12 KERNEL32!BaseThreadInitThunk+0x14
13 ntdll!RtlUserThreadStart+0x21

PrintDialog!<lambda_361a11138f2d753fa3792d41da618c5f>::operator()+0x384:
00007ffc`9c992594 cc int 3
@r14 this = 0x0000027f`ef4a0788
000000cf`11bff690 **bindPrinterActivity** = class PrintDialogTelemetry::**BindPrinterActivity**

((PrintDialog!PrintDialog::DataModel::DeviceModel *)0x27fef144e10) : 0x27fef144e10
[+0x028] _deviceId : 0x27fef05ce50 : \\?\SWD#PRINTENUM#{7C5B9B89-B6EE-4955-AAE0-B6A61B83D065}#{0ecef634-6ef0-472a-8085-5ad023ecbccd}
[+0x030] _deviceName : 0x27fef0705c0 : "Pantum CP2257DN HBP" [Type: Platform::String *]
[+0x038] _displayName : 0x27fef06fd00 : "Pantum CP2257DN HBP" [Type: Platform::String *]

PrintDialog!wil::details::ReportFailure:
000000cf`11bff5c8 hr = 0x**80004005**

Photo TTD:
DbgID ThreadID User Kernel Position Approx. System Time

2 2808 (0n10248) 0s 0s 00097EF2:0000 Thursday, January 11, 2024 2:56:56.440 AM

```
# Call Site                                                                    Info
0 ntdll!RtlRaiseException+0x0
1 ntdll!vDbgPrintExWithPrefixInternal+0x232
2 ntdll!DbgPrint+0x3c
3 KERNELBASE!OutputDebugStringA+0x1b6
4 schk_x64!UnSetWinHook+0x3067
5 schk_x64+0x263c3
6 prntvpt!PTOpenProviderExImp+0x96
7 prntvpt!PTOpenProviderImp+0x37
8 prntvpt!CPrintTicketServerBase::Bind+0x1c
9 prntvpt!PTOpenProvider+0xfb
a PrintPlatformConfig!PrintPlatform::HPTProviderRAII::{ctor}+0x20
b PrintPlatformConfig!PrintPlatform::MergePrintTicketWithDefault+0x159
c PrintPlatformConfig!<lambda_ac9c7b545bc881a9f3b8336bf076cb3a>::operator()+0xbb
d
PrintPlatformConfig!PrintCore::CaptureAndConvertExceptionToHR<<lambda_ac9c7b545bc881a
9f3b8336bf076cb3a> >+0x17
e
PrintPlatformConfig!PrintPlatform::PrintPlatformPrintSchemaFactoryLegacy::CreatePrintSchema
Ticket+0x12c
f
Windows_Graphics_Printing!Windows::Graphics::Printing::OptionDetails::PrintTaskOptionDetail
sServer::PrintTaskOptionsServerTransaction::BindPrinter+0x2bd
10
Windows_Graphics_Printing!Windows::Graphics::Printing::PrintTaskServer::PrintTaskServerPriv:
:BindPrinter+0x241
11 RPCRT4!Invoke+0x73
12 RPCRT4!Ndr64StubWorker+0xb4a
13 RPCRT4!NdrStubCall3+0xc9
14 combase!CStdStubBuffer_Invoke+0x5f
15 RPCRT4!CStdStubBuffer_Invoke+0x3b
16
combase!InvokeStubWithExceptionPolicyAndTracing::__l6::<lambda_76d9e92c799d246a4afbe6
4a2bf5673d>::operator()+0x18
17
combase!ObjectMethodExceptionHandlingAction<<lambda_76d9e92c799d246a4afbe64a2bf56
73d> >+0x43
18 combase!InvokeStubWithExceptionPolicyAndTracing+0xa8
19 combase!DefaultStubInvoke+0x1c4
1a combase!SyncStubCall::Invoke+0x22
1b combase!SyncServerCall::StubInvoke+0x26
1c combase!StubInvoke+0x265
1d combase!ServerCall::ContextInvoke+0x435
1e combase!CServerChannel::ContextInvoke+0x70
1f combase!DefaultInvokeInApartment+0xad
20 combase!AppInvoke+0x200
```

21 combase!ComInvokeWithLockAndIPID+0xc17
22 combase!ThreadInvoke+0x1f60
23 RPCRT4!DispatchToStubInCNoAvrf+0x18
24 RPCRT4!RPC_INTERFACE::DispatchToStubWorker+0x1a0
25 RPCRT4!RPC_INTERFACE::DispatchToStub+0x98
26 RPCRT4!RPC_INTERFACE::DispatchToStubWithObject+0x160
27 RPCRT4!LRPC_SBINDING::DispatchToStubWithObject+0x1f
28 RPCRT4!LRPC_SCALL::DispatchRequest+0x16f
29 RPCRT4!LRPC_SCALL::QueueOrDispatchCall+0x125
2a
RPCRT4!LRPC_SCALL::HandleRequest+0x7fa Clie
nt: PID: 0x20f8 TID: 0x25d8
2b RPCRT4!LRPC_SASSOCIATION::HandleRequest+0x200
2c RPCRT4!LRPC_ADDRESS::HandleRequest+0x341
2d RPCRT4!LRPC_ADDRESS::ProcessIO+0x8a2
2e RPCRT4!LrpcIoComplete+0xc5
2f ntdll!TppAlpcpExecuteCallback+0x260
30 ntdll!TppWorkerThread+0x3c8
31 KERNEL32!BaseThreadInitThunk+0x14
32 ntdll!RtlUserThreadStart+0x21

DbgID ThreadID User Kernel Position Approx. System Time
2 2808 (0n10248) 0s 0s 003F89C1:0000 Thursday, January 11, 2024 2:57:14.147 AM

Call Site
0 ntdll!RtlRaiseException+0x0
1 ntdll!vDbgPrintExWithPrefixInternal+0x232
2 ntdll!DbgPrint+0x3c
3 KERNELBASE!OutputDebugStringA+0x1b6
4 **schk_x64!UnSetWinHook**+0x3067
5 schk_x64+0x25533
6 UNIDRVUI!UniDrvUI::CalculatePrintableArea+0xd8
7 UNIDRVUI!UniDrvUI::CoreDriverPrintableArea+0x76
8 UNIDRVUI!UniDrvUI::CPrintTicketProvider::GenerateCoreDriverPrintCapabilities+0x338
9 UNIDRVUI!UniDrvUI::CPrintTicketProvider::GetPrintCapabilities+0x9c
a prntvpt!PTGetPrintCapabilitiesImp+0x128
b prntvpt!TProviderInfo::GetSupportedFeaturesList+0x65
c prntvpt!PTMergeAndValidatePrintTicketImp+0x1bf
d prntvpt!CPrintTicketServerBase::MergeAndValidatePrintTicket+0x9f
e prntvpt!PTMergeAndValidatePrintTicket+0x99
f PrintPlatformConfig!PrintPlatform::MergePrintTicketWithDefault+0x236
10 PrintPlatformConfig!<lambda_ac9c7b545bc881a9f3b8336bf076cb3a>::operator()+0xbb
11
PrintPlatformConfig!PrintCore::CaptureAndConvertExceptionToHR<<lambda_ac9c7b545bc881a
9f3b8336bf076cb3a> >+0x17

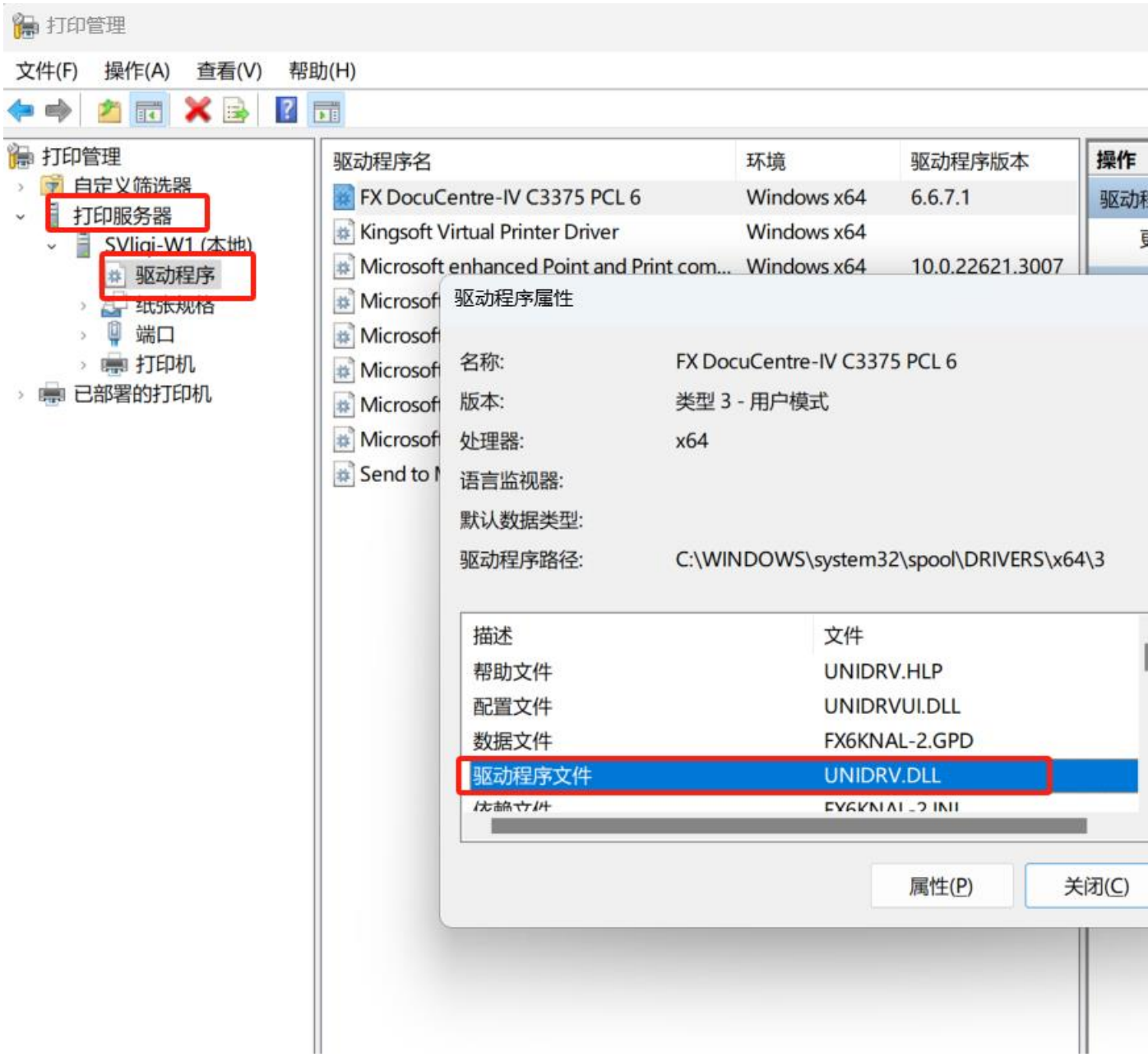
Browse full module list
start end module name

```
00007ffc`9d130000 00007ffc`9d1b5000   schk_x64   (export symbols)       schk_x64.dll
    Loaded symbol image file: schk_x64.dll
    Image path: C:\WINDOWS\System32\schk_x64.dll
    Image name: schk_x64.dll
    Browse all global symbols  functions  data
    Timestamp:        Fri Feb  3 11:25:24 2023 (63DC7EA4)
    CheckSum:         0008F525
    ImageSize:        00085000
    File version:     6.0.0.0
    Product version:  6.0.0.0
    File flags:       0 (Mask 3F)
    File OS:          40004 NT Win32
    File type:        2.0 Dll
    File date:        00000000.00000000
    Translations:     0404.04b0
    Information from resource tables:
        CompanyName:
        ProductName:      GSC Desktop terminal security management platform
        InternalName:
        OriginalFilename:
        ProductVersion:   6.0.0.0
        FileVersion:      6.0.0.0
        PrivateBuild:
        SpecialBuild:
        FileDescription:  GSC FILE
        LegalCopyright:   (C)GeneralSoft Corporation. All rights reserved.
```

===下一步方案===

1.临时卸载 TMS，查看 photo 中使用 Pantum CP2257DN HBP 打印预览是否仍有异常

2.若第一步方案执行后仍有异常，检查环境中使用 UNIDRV.dll 的打印机是否有在 photo 打印预览好的场景，关于查看打印机是否用到 UNIDRV.dll，您可参考如下 Print Management 截图，具体方法为：按 Win+R，在输入框中输入“printmanagement.msc”，点击“打印服务器”-“本地”-“驱动程序”，右键选择右侧列表中打印机的“属性”，查看驱动程序文件，是否为 UNIDRV.DLL



3.若存在使用 UNIDRV.dll， photo 程序打印预览好的打印机选项，我们需要对此场景捕获一份 TTD（printdialog+photo）做为好的基准以做比对，另外移除 schk_x64 驱动后还有问题的话，也请同步再上传一份问题场景 TTD（printdialog+photo）

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

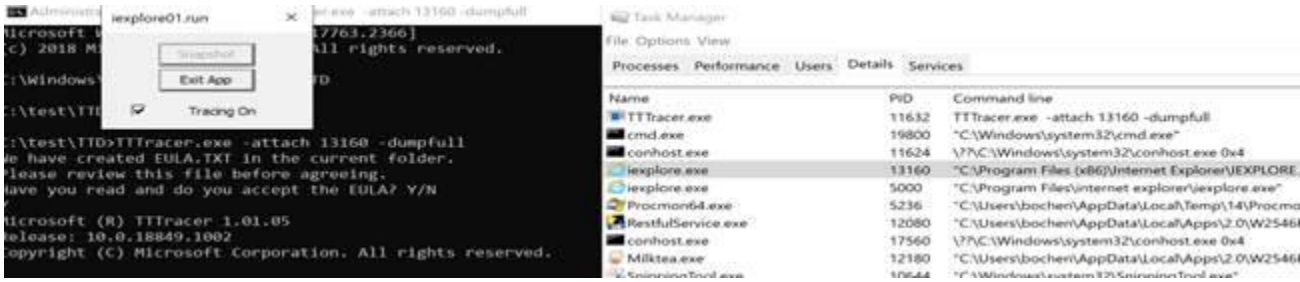
发件人: Li Qi
发送时间: 2024 年 1 月 11 日 10:29
收件人: '张' <1257503651@qq.com>; '唐晨明' <tangchenming_cz@js.icbc.com.cn>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>; ICBC 案例通知 <win10sup@sdc.icbc.com.cn>
主题: 回复: 回复: [案例号: CAS-10387-B9Z9T1] % |P2|ICBC|工行反馈在 V2020-L 版本安装 KB5030214 补丁后打印异常 % 初次响应 CMIT:0001601

您好:
当前问题的关键点在于 printdialog 进程的行为，但我们此次抓取的日志并未包含相关信息，所以可能还需要咱们再重新抓取一次，好的场景和坏的场景我们分开抓取，每个场景包括: TTD+procmon 两部分。请按照如下步骤操作:

---好的场景---
1. 打开 photo，调出打印窗口，这时候 Microsoft.photo 进程的 PID 和 PrintDialog 进程的 PID 均可从任务管理器中查看到
2.管理员打开两个 cmd 窗口，分别执行如下指令，同时开启 Microsoft.photo 进程和 PrintDialog 进程的 TTD

```
tttracer -attach <PID> -dumpfull
```

等待小窗口弹出，如下实例以 iexplorer 为例



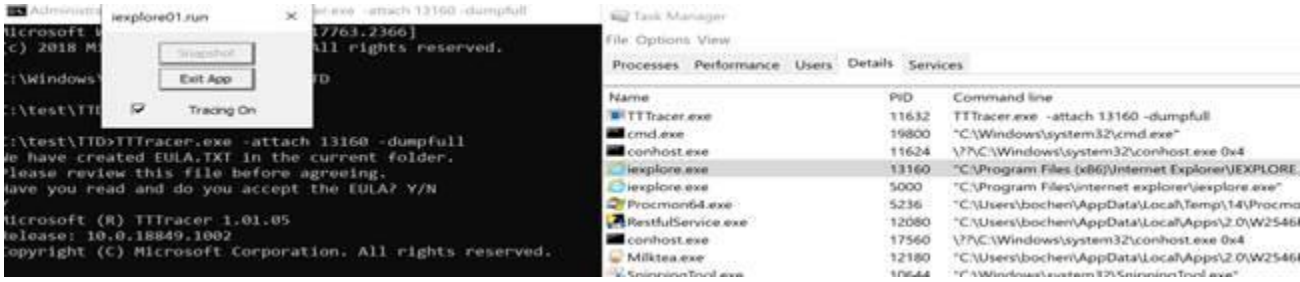
3.开启 procmon
4.**切换至可成功打印的打印机**
5.停止 procmon 并**取消勾选弹出窗口的"tracing on" 选框即可（应该有两个进程的选框，分别取消）**，然后 tttrace 就会自动停止，并执行如下命令确认 tttracer 已停止
tttracer.exe -stop all tttracer.exe -delete all

---坏的场景---
1. 打开 photo，调出打印窗口，这时候 Microsoft.photo 进程的 PID 和 PrintDialog 进程的 PID 均可从任务管理器中查看到

2.管理员打开两个 cmd 窗口，分别执行如下指令，同时开启 Microsoft.photo 进程和 PrintDialog 进程的 TTD

```
tttracer -attach <PID> -dumpfull
```

等待小窗口弹出，如下实例以 iexplorer 为例



3.开启 procmon

4.**切换至失败闪退的打印机**（若程序自动退出，则可能 TTD 会自动停止）

5.停止 procmon 并**取消勾选弹出窗口的“tracing on” 选框即可（应该有两个进程的选框，分别取消）**，然后 tttrace 就会自动停止，并执行如下命令确认 tttracer 已停止

tttracer.exe -stop all tttracer.exe -delete all

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: 2023 年 12 月 25 日 13:19
收件人: '张' <1257503651@qq.com>; '唐晨明' <tangchenming_cz@js.icbc.com.cn>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>; ICBC 案例通知 <win10sup@sdc.icbc.com.cn>
主题: 回复: 回复： [案例号: CAS-10387-B9Z9T1] % |P2|ICBC|工行反馈在 V2020-L 版本安装 KB5030214 补丁后打印异常 % 初次响应 CMIT:0001601

您好:
请问您是否有电话方便沟通？方便的话可以留下您的电话，以便我和您联系。关于您提到的问题，请参照以下内容:

1. tttracer -onlaunch PrintDiaglog.exe -out c:/temp/指令执行后没有弹出采集框，也没有日志文件在 temp 生成。

   -onlaunch 参数是指在 PrintDiaglog 进程开始启动时进行采集，在我们之前收集的日志中，该进程在出现打印错误阶段才会开启，因此他并不是第一时间开启，直到出现问题前才会出现采集框。此时在问题出现后取消勾选 tracing on 才会记录该进程的日志信息。

2. tttracer -attach pid -dumpfull 指令采集不能正常打印机时会出现闪退的现象，照片进程被直接关闭，不确定采集是否成功。

   您说的这个情况只发生在正常打印机的场景下么？是在取消勾选 tracing on 之前出现闪退和进程关闭的情况还是之后？

3. 采集日志文件过大，单个文件 5g 左右

   由于我们现在抓取的无论是.run 还是.etl 还是.pml 文件都是问题复现整个过程的记录日志，因此确实可能出现您说的这种情况，这与您的复现操作时间有关，是正常的，您可以在全部收取之后进行分卷压缩再上传或者您可以提供其他的上传地址给我，我再想办法下载。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: 张 <1257503651@qq.com>
发送时间: 2023 年 12 月 22 日 14:56
收件人: Li Qi <liqi@cmgos.com>
主题: 回复： [案例号: CAS-10387-B9Z9T1] % |P2|ICBC|工行反馈在 V2020-L 版本安装 KB5030214 补丁后打印异常 % 初次响应 CMIT:0001601

您好，采集日志时候遇到几个问题

1. tttracer -onlaunch PrintDiaglog.exe -out c:/temp/指令执行后没有弹出采集框，也没有日志文件在 temp 生成。

2. tttracer -attach pid -dumpfull 指令采集不能正常打印机时会出现闪退的现象，照片进程被直接关闭，不确定采集是否成功。

3. 采集日志文件过大，单个文件 5g 左右

---------- 原始邮件 ----------

发件人: Li Qi <liqi@cmgos.com>
发送时间: 2023 年 12 月 20 日 16:35
收件人: 张 <1257503651@qq.com>, 唐晨明 <tangchenming_cz@js.icbc.com.cn>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>, ICBC 案例通知 <win10sup@sdc.icbc.com.cn>
主题: 回复: [案例号: CAS-10387-B9Z9T1] % |P2|ICBC|工行反馈在 V2020-L 版本安装 KB5030214 补丁后打印异常 % 初次响应 CMIT:0001601

唐女士，您好：

如刚才电话沟通，接下来我们还是需要重新收取下以下场景的日志，即：安装补丁后，不同打印机正常打印和异常打印的过程的对比日志，分别记录下打印机的型号和操作时间。**要求：在同一 photo 应用的窗口进程下切换不同的打印机场景**

需要收集的日志有如下三类，分别是：ETL，Procmon，TTD，请按以下步骤执行。

1， 在 C 盘新建一个目录 (**C:\mstrace**)，将之前的 Process Monitor 工具解压后拷贝到 C:\mstrace；再在 C 盘新建一个目录(**c:\temp**)，为之后收取 TTD 做准备

2. **ETL 和 procmon 的日志收集工作：**
   以管理员打开一个 CMD（或者将附件的 txt 文件，更改后缀为 bat 后，以管理员身份执行也可以），输入以下的命令开启日志收集：

```
cd /d C:\mstrace
procmon /backingfile C:\mstrace\logfile.pml /AcceptEula /Minimized /Quiet

logman create trace "printscan_print1" -ow -o c:\printscan_print1.etl -p "Microsoft-Windows-PrintService" 0xffffffffffffffff 0xff -nb 16 16 -bs 1024 -mode Circular -f bincirc -max 4096 -ets

logman update trace "printscan_print1" -p {C9BF4A08-D547-4D11-8242-E03A18B5BE01} 0xffffffffffffffff 0xff -ets

logman update trace "printscan_print1" -p {C9BF4A01-D547-4D11-8242-E03A18B5BE01} 0xffffffffffffffff 0xff -ets
```

```
logman update trace "printscan_print1" -p {C9BF4A06-D547-4D11-8242-E03A18B5BE01} 0xffffffffffffffff 0xff -ets

logman update trace "printscan_print1" -p {C9BF4A04-D547-4D11-8242-E03A18B5BE01} 0xffffffffffffffff 0xff -ets

logman update trace "printscan_print1" -p {C9BF4A02-D547-4D11-8242-E03A18B5BE01} 0xffffffffffffffff 0xff -ets

logman update trace "printscan_print1" -p {C9BF4A03-D547-4D11-8242-E03A18B5BE01} 0xffffffffffffffff 0xff -ets

logman update trace "printscan_print1" -p {C9BF4A9F-D547-4D11-8242-E03A18B5BE01} 0xffffffffffffffff 0xff -ets

logman update trace "printscan_print1" -p {C9BF4A9E-D547-4D11-8242-E03A18B5BE01} 0xffffffffffffffff 0xff -ets

logman update trace "printscan_print1" -p {C9BF4A05-D547-4D11-8242-E03A18B5BE01} 0xffffffffffffffff 0xff -ets

logman update trace "printscan_print1" -p {EE7E960D-5E42-4C28-8F61-D8FA8B0DD84D} 0xffffffffffffffff 0xff -ets

logman update trace "printscan_print1" -p {CE444D6A-F287-4977-BBBD-89A0DD65B71D} 0xffffffffffffffff 0xff -ets

logman update trace "printscan_print1" -p {D34AE79A-15FB-44F9-9FD8-3098E6FFFD49} 0xffffffffffffffff 0xff -ets

logman update trace "printscan_print1" -p {27239FD0-425E-11D8-9E39-000039252FD8} 0xffffffffffffffff 0xff -ets

logman update trace "printscan_print1" -p {F4DF4FA4-66C2-4C14-ABB1-19D099D7E213} 0xffffffffffffffff 0xff -ets

logman update trace "printscan_print1" -p {7663DA2F-1594-4C33-83DD-D5C64BBED68A} 0xffffffffffffffff 0xff -ets

logman update trace "printscan_print1" -p {AAED978E-5B0C-4F71-B35C-16E9C0794FF9} 0xffffffffffffffff 0xff -ets
```

```
logman update trace "printscan_print1" -p {9677DFEF-EACF-4173-8977-FFB0086B11E6} 0xffffffffffffffff 0xff -ets

logman update trace "printscan_print1" -p "Microsoft-Windows-PrintBRM" 0xffffffffffffffff 0xff -ets

logman update trace "printscan_print1" -p {301CCC25-D58B-4C5E-B6A5-15BCF8B0077F} 0xffffffffffffffff 0xff -ets

logman update trace "printscan_print1" -p {C9BF4A9E-D547-4D11-8242-E03A18B5BEEE} 0xffffffffffffffff 0xff -ets

logman update trace "printscan_print1" -p {04160794-60B6-4EC7-96FF-4953691F94AA} 0xffffffffffffffff 0xff -ets

logman update trace "printscan_print1" -p {3EA31F33-8F51-481D-AEB7-4CA37AB12E48} 0xffffffffffffffff 0xff -ets

logman update trace "printscan_print1" -p "Microsoft-Windows-Spooler-LPDSVC" 0xffffffffffffffff 0xff -ets

logman update trace "printscan_print1" -p {9E6D0D9B-1CE5-44B5-8B98-F32ED89077EC} 0xffffffffffffffff 0xff -ets

logman update trace "printscan_print1" -p {F30FAB8E-84BB-48D4-8E80-F8967EF0FE6A} 0xffffffffffffffff 0xff -ets

logman update trace "printscan_print1" -p "Microsoft-Windows-Spooler-LPRMON" 0xffffffffffffffff 0xff -ets

logman update trace "printscan_print1" -p {5ED940EB-18F9-4227-A454-8EF1CE5B3272} 0xffffffffffffffff 0xff -ets

logman update trace "printscan_print1" -p {99F5F45C-FD1E-439F-A910-20D0DC759D28} 0xffffffffffffffff 0xff -ets

logman update trace "printscan_print1" -p "Microsoft-Windows-SpoolerTCPMon" 0xffffffffffffffff 0xff -ets

logman update trace "printscan_print1" -p {62A0EB6C-3E3E-471D-960C-7C574A72534C} 0xffffffffffffffff 0xff -ets
```

```
logman update trace "printscan_print1" -p {9558985E-3BC8-45EF-A2FD-2E6FF06FB886} 0xffffffffffffffff 0xff -ets

logman update trace "printscan_print1" -p {836767A6-AF31-4938-B4C0-EF86749A9AEF} 0xffffffffffffffff 0xff -ets

logman update trace "printscan_print1" -p {7672778D-86FE-41D0-85C8-82CAA8CE6168} 0xffffffffffffffff 0xff -ets

logman update trace "printscan_print1" -p {6D1E0446-6C52-4B85-840D-D2CB10AF5C63} 0xffffffffffffffff 0xff -ets

logman update trace "printscan_print1" -p {B795C7DF-07BC-4362-938E-E8ABD81A9A01} 0xffffffffffffffff 0xff -ets

logman update trace "printscan_print1" -p {09737B09-A25E-44D8-AA75-07F7572458E2} 0xffffffffffffffff 0xff -ets

logman update trace "printscan_print1" -p {34F7D4F8-CD95-4B06-8BF6-D929DE4AD9DE} 0xffffffffffffffff 0xff -ets

logman update trace "printscan_print1" -p {B42BD277-C2BA-468B-AB3D-05B1A1714BA3} 0xffffffffffffffff 0xff -ets

logman update trace "printscan_print1" -p {A83C80B9-AE01-4981-91C6-94F00C0BB8AA} 0xffffffffffffffff 0xff -ets

logman update trace "printscan_print1" -p {EB4C6075-0B67-4A79-A0A3-7CD9DF881194} 0xffffffffffffffff 0xff -ets

logman update trace "printscan_print1" -p {0ED38D2B-4ACC-4E23-A8EC-D0DACBC34637} 0xffffffffffffffff 0xff -ets

logman update trace "printscan_print1" -p {301CCC25-D58B-4C5E-B6A5-15BCF8B0077F} 0xffffffffffffffff 0xff -ets

logman update trace "printscan_print1" -p {C9BF4A9E-D547-4D11-8242-E03A18B5BEEE} 0xffffffffffffffff 0xff -ets

logman update trace "printscan_print1" -p {3EA31F33-8F51-481D-AEB7-4CA37AB12E48} 0xffffffffffffffff 0xff -ets
```

```
logman update trace "printscan_print1" -p "Microsoft-Windows-Spooler-LPDSVC" 0xffffffffffffffff 0xff -ets
```

3， TTD 启动

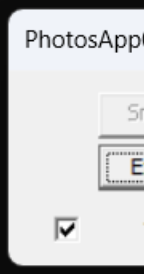
管理员身份打开 cmd，跳转到 TTD 工具的解压路径，运行如下两条指令，其中 PID 需替换成 **Microsoft.Photo.exe（您的电脑上显示的照片应用版本的进程名称）**的进程 ID（任务管理器-详细信息中查看）

详细信息　　运行新任务　　结束任务

名称	PID	状态	用户名	CPU	内存(活动...	句柄	体系结构
Microsoft.Flow.RPA.LogShip...	6720	正在运行	NETWOR...	00	10,636 K	747	x64
Microsoft.Flow.RPA.Update...	6772	正在运行	SYSTEM	00	9,728 K	599	x64
Microsoft.SharePoint.exe	13068	正在运行	liqi	00	1,856 K	504	x64
mmcrashpad_handler64.exe	13332	正在运行	liqi	00	184 K	157	x64
MsMpEng.exe	6736	正在运行	SYSTEM	00	2,180 K	701	x64
MSPCManagerService.exe	6256	正在运行	SYSTEM	00	26,288 K	1,107	x64
nac_agent.exe	7600	正在运行	SYSTEM	00	2,560 K	264	x86
nac_monitor.exe	6180	正在运行	SYSTEM	00	404 K	93	x86
OfficeClickToRun.exe	5708	正在运行	SYSTEM	00	4,704 K	805	x64
OneApp.IGCC.WinService.exe	5956	正在运行	SYSTEM	00	2,492 K	722	x64
OUTLOOK.EXE	6884	正在运行	liqi	00	245,276 K	7,280	x64
PhoneExperienceHost.exe	14608	正在运行	liqi	00	3,480 K	1,451	x64
PhotosApp.exe	2724	正在运行	liqi	00	62,584 K	1,360	x64
PhotosService.exe	9772	正在运行	liqi	00	3,052 K	369	x64
PopBlock.exe	12760	正在运行	liqi	00	3,424 K	270	x86
PowerMgr.exe	11604	正在运行	liqi	00	1,512 K	393	x86
PresentationFontCache.exe	11440	正在运行	LOCAL SE...	00	428 K	255	x64
QQProtect.exe	6232	正在运行	SYSTEM	00	1,852 K	484	x86
RayLinkCapturer.exe	9912	正在运行	SYSTEM	00	448 K	253	x64
RayLinkCapturer.exe	10404	正在运行	SYSTEM	00	484 K	253	x64
RayLinkService.exe	6268	正在运行	SYSTEM	00	2,240 K	332	x64

```
tttracer -attach <PID> -dumpfull
```

```
C:\Users\liqi\Downloads\CAS-10387-B9Z9T1\TTD>tttracer -attach 11088 -
Microsoft (R) TTTracer 1.01.05
Release: 10.0.18849.1002
Copyright (C) Microsoft Corporation. All rights reserved.
```



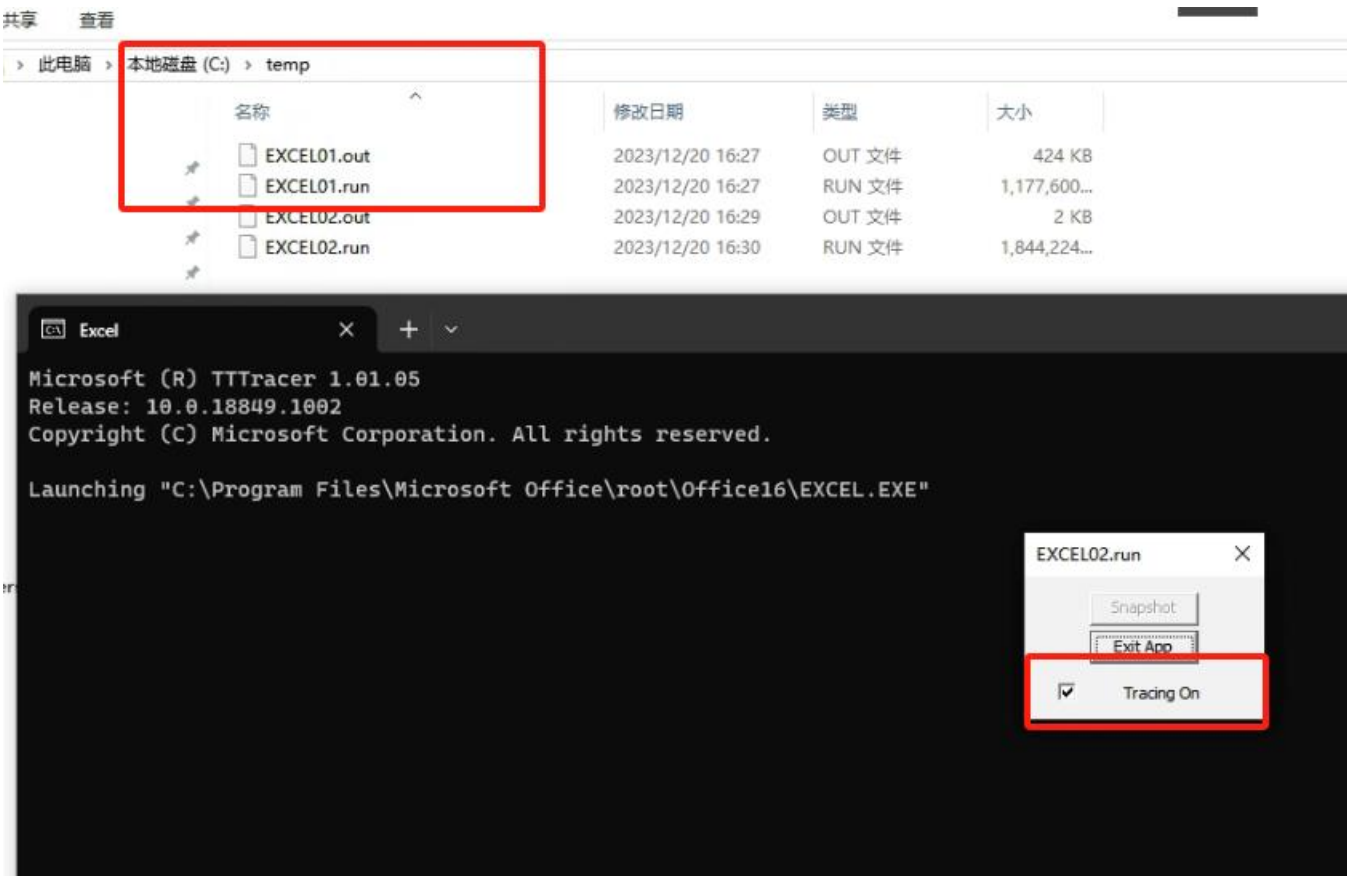
tttracer -onlaunch PrintDiaglog.exe -out c:\temp\

4， 复现问题（打印问题，要求：在同一 photo 应用的窗口进程下切换不同的打印机场景）

5， TTD 停止

取消勾选弹出窗口的“tracing on” 选框即可（应该有两个进程的选框，分别取消）

```
PhotosApp.exe(x64) (PID:11088): Tracing stopped after 237812ms
  Full trace dumped to C:\Users\liqi\Downloads\CAS-10387-B9Z9T1\TTD\Ph
```



tttracer 此时会自动停止，并执行如下命令确认 tttracer 已停止

```
tttracer.exe -stop all
tttracer.exe -delete all
```

6， 运行以下命令行**停止并收集 procmon 和 ETL 日志：**

```
procmon /terminate
logman stop "printscan_print1" -ets
```

7， 在客户端上以管理员方式运行 CMD，并输入下面的命令**收集系统日志：**

```
msinfo32 /nfo C:\mstrace\SYSSUM.NFO /categories +systemsummary
wevtutil epl System C:\mstrace\system.evtx
wevtutil epl Application C:\mstrace\app.evtx
```

```
wmic qfe list > C:\mstarce\1.txt

gpresult /h c:\mstrace\gp.html
```

最后，将 TTD 文件夹中的.run 文件，c 盘 temp 文件夹中的.run 文件和 c:\mstrace 文件夹压缩后发送给我分析，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: 2023 年 12 月 14 日 11:23
收件人: ’张’ <1257503651@qq.com>; ’唐晨明’ <tangchenming_cz@js.icbc.com.cn>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>; ICBC 案例通知 <win10sup@sdc.icbc.com.cn>
主题: 回复: [案例号: CAS-10387-B9Z9T1] % |P2|ICBC|工行反馈在 V2020-L 版本安装 KB5030214 补丁后打印异常 % 初次响应 CMIT:0001601

您好：

已收到您的附件，请将我上封邮件中提到的 CMGELogCollector 收集的日志也一并传给我吧，谢谢

请下载工具 CMGELogCollectorV2 至本地，下载路径为：
https://cduc.cmgos.com/download.php?id=1178&token=yvIIzaJT9PWSwYJbjqGWnX8oMzqEkJaw

点击“收集”按钮，收集系统日志并发送给我，谢谢。具体步骤如下：

CMGELogCollector：

解压后运行 CMGELogCollector.exe，保持默认勾选，点击“收集”，运行几分钟后会在桌面**生成日志压缩包**。

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：张 <1257503651@qq.com>
发送时间：2023 年 12 月 13 日 16:45
收件人：Li Qi <liqi@cmgos.com>
主题：回复：回复：回复：转发：【外来邮件，注意核实】回复：[案例号：CAS-10387-B9Z9T1] % |P2|ICBC|工行反馈在 V2020-L 版本安装 KB5030214 补丁后打印异常 % 初次响应 CMIT:0001601

安装新版驱动后依然无法打印，采集了两个日志，成功为正常打印日志，失败为无法打印日志。

从 QQ 邮箱发来的超大附件

Logfile(失败).PML (116.73M, 2024 年 01 月 12 日 16:38 到期)

进入下载页面：https://mail.qq.com/cgi-bin/ftnExs_download?k=2234373762588d9ec7cfc47d15380b491c40525350095a00490d0f5203150a515d521a550b01084b5100060655595f56505002513329392a0b53515e5f5d11acc384eb1e1d68742a6409&t=exs_ftn_download&code=d477389f

Logfile(成功).PML (235.58M, 2024 年 01 月 12 日 16:38 到期)

进入下载页面：https://mail.qq.com/cgi-bin/ftnExs_download?k=2462316145d822c7c199c22b166156191a16555552515d534f540258564c525503001c075257531b07040150535050545706075130706 47a0d0557085c044c85abdb97481e31297a625f&t=exs_ftn_download&code=bb1a0ad6