

许先生 您好:

感谢您的电话接听。

确认您的问题已经解决，我将归档此案例。

工单的归档并不会影响我们为您提供技术支持服务，如您有其他问题，您可以致电技术支持热线 4008180055。

案例总结:

问题定义:

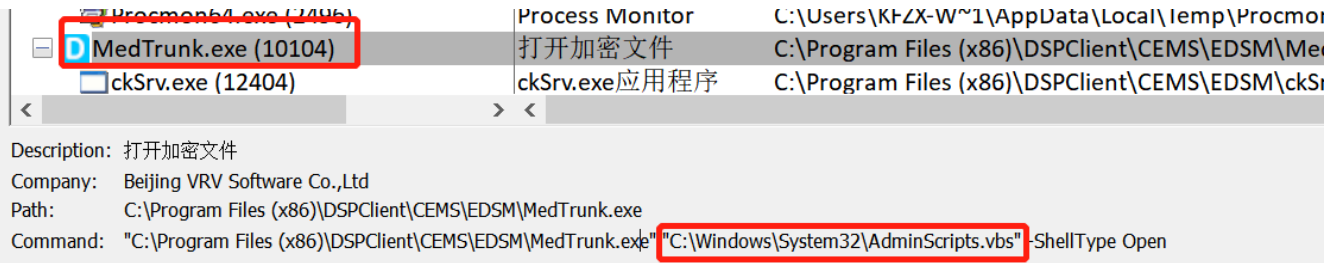
用户反馈设备登录时 AdminScripts.vbs 脚本运行提示找不到指定路径，需要协助分析。

问题总结:

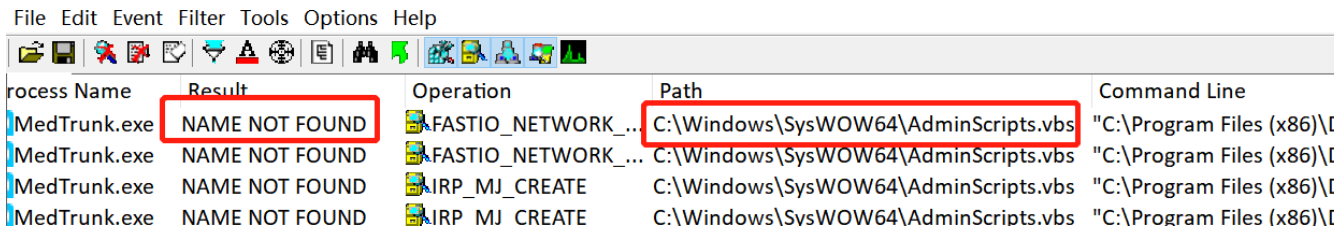
用户联系第三方应用 DSP 厂商确认是 MedTrunk.exe 导致的问题，新版应用已经修复了这个问题，可以关闭案例。

问题具体分析:

查看对应的 procmon 日志，（AdminScripts.vbs 在 C:\Windows\system32 目录）可以看到 DSP 应用 MedTrunk.exe 加载启动了 AdminScripts.vbs 脚本。



在启动过程中要去查询 C:\Windows\sysWOW64\AdminScripts.vbs 脚本，但是找不到此脚本，结果出现弹窗错误。



请第三方应用 DSP 厂商排查为什么 MedTrunk.exe 加载启动 C:\Windows\system32\下的 vbs 脚本
本会重定向到 C:\Windows\sysWOW64\目录查找对应脚本。

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

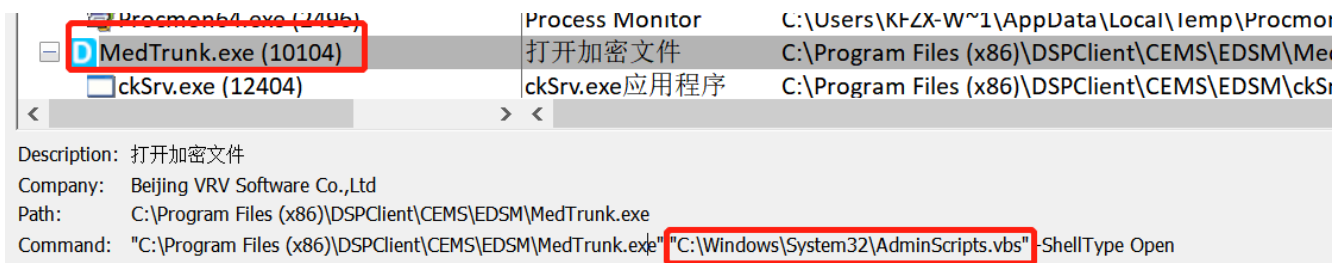


发件人: Wei Liang
发送时间: 2023 年 1 月 31 日 15:03
收件人: '许翔' <win10sup@sdicbc.com.cn>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: [案例号: CAS-08073-F5Y7B2] % |P2||ICBC|运行脚本报找不到指定路径 % 初次响应 CMIT:0001186

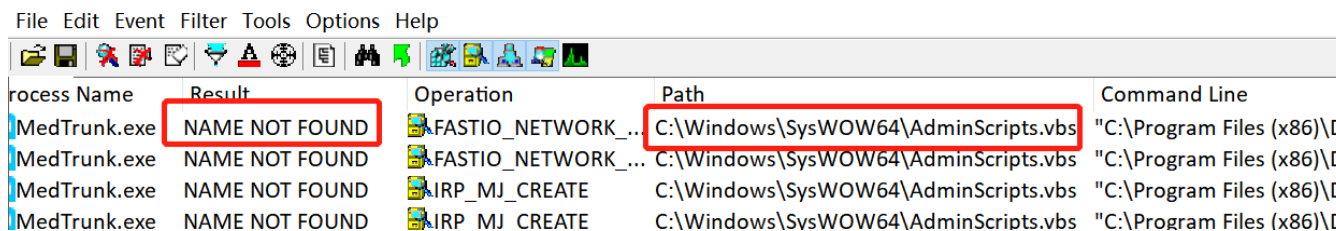
许先生 您好:

感谢您的电话接听。

查看脚本运行失败的 procmon 日志，（AdminScripts.vbs 在 C:\Windows\system32 目录）可以看到 DSP 应用 MedTrunk.exe 加载启动了 AdminScripts.vbs 脚本。

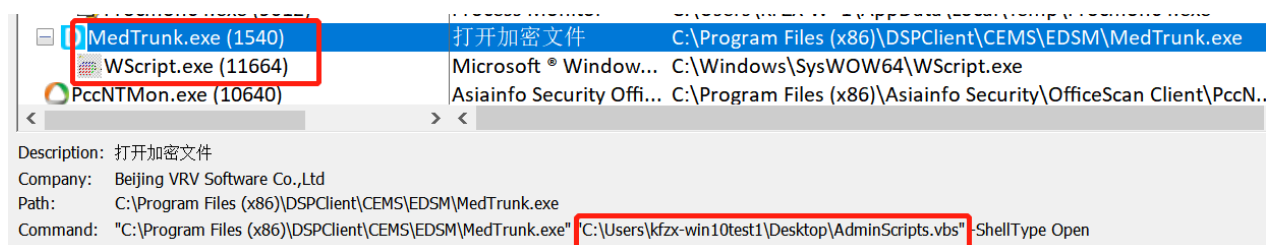


在启动过程中要去查询 C:\Windows\sysWOW64\AdminScripts.vbs 脚本，但是找不到此脚本，结果出现弹窗错误。



Process Name	Result	Operation	Path	Command Line
MedTrunk.exe	NAME NOT FOUND	FASTIO_NETWORK_...	C:\Windows\SysWOW64\AdminScripts.vbs	"C:\Program Files (x86)\D...
MedTrunk.exe	NAME NOT FOUND	FASTIO_NETWORK_...	C:\Windows\SysWOW64\AdminScripts.vbs	"C:\Program Files (x86)\D...
MedTrunk.exe	NAME NOT FOUND	IRP_MJ_CREATE	C:\Windows\SysWOW64\AdminScripts.vbs	"C:\Program Files (x86)\D...
MedTrunk.exe	NAME NOT FOUND	IRP_MJ_CREATE	C:\Windows\SysWOW64\AdminScripts.vbs	"C:\Program Files (x86)\D...

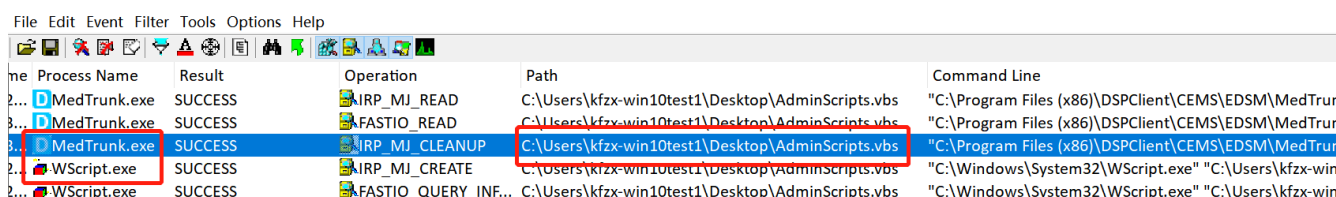
而正常启动 vbs 脚本的 procmon 日志，（AdminScripts.vbs 在当前登录用户的桌面目录）同样可以看到 DSP 应用 MedTrunk.exe 加载启动了 AdminScripts.vbs 脚本。



Process Name	Result	Operation	Path	Command Line
MedTrunk.exe (1540)	SUCCESS	打开加密文件	C:\Program Files (x86)\DSPClient\CEMS\EDSM\MedTrunk.exe	
WScript.exe (11664)	SUCCESS	Microsoft® Window...	C:\Windows\SysWOW64\WScript.exe	
PccNTMon.exe (10640)	SUCCESS	Asiainfo Security Offi...	C:\Program Files (x86)\Asiainfo Security\OfficeScan Client\PccN...	

Description: 打开加密文件
Company: Beijing VRV Software Co.,Ltd
Path: C:\Program Files (x86)\DSPClient\CEMS\EDSM\MedTrunk.exe
Command: "C:\Program Files (x86)\DSPClient\CEMS\EDSM\MedTrunk.exe" "C:\Users\kfzx-win10test1\Desktop\AdminScripts.vbs" -ShellType Open

但因为此时 AdminScripts.vbs 脚本不在 C:\Windows\system32\目录，MedTrunk.exe 读取到指定目录下的 AdminScripts.vbs 脚本，并调用 WScript.exe 运行 vbs 脚本。



Process Name	Result	Operation	Path	Command Line
MedTrunk.exe	SUCCESS	IRP_MJ_READ	C:\Users\kfzx-win10test1\Desktop\AdminScripts.vbs	"C:\Program Files (x86)\DSPClient\CEMS\EDSM\MedTrunk.exe"
MedTrunk.exe	SUCCESS	FASTIO_READ	C:\Users\kfzx-win10test1\Desktop\AdminScripts.vbs	"C:\Program Files (x86)\DSPClient\CEMS\EDSM\MedTrunk.exe"
MedTrunk.exe	SUCCESS	IRP_MJ_CLEANUP	C:\Users\kfzx-win10test1\Desktop\AdminScripts.vbs	"C:\Program Files (x86)\DSPClient\CEMS\EDSM\MedTrunk.exe"
WScript.exe	SUCCESS	IRP_MJ_CREATE	C:\Users\kfzx-win10test1\Desktop\AdminScripts.vbs	"C:\Windows\System32\WScript.exe" "C:\Users\kfzx-win10test1\Desktop\AdminScripts.vbs"
WScript.exe	SUCCESS	FASTIO_QUERY_INF...	C:\Users\kfzx-win10test1\Desktop\AdminScripts.vbs	"C:\Windows\System32\WScript.exe" "C:\Users\kfzx-win10test1\Desktop\AdminScripts.vbs"

针对此问题的建议如下：

- 1) 调整域控上的 AdminScripts.vbs 脚本推送策略，将此脚本推送到 C:\Windows\目录，而不是 C:\Windows\system32\目录。
- 2) 或者请三方应用 DSP 厂商排查为什么 MedTrunk.exe 加载启动 C:\Windows\system32\下的 vbs 脚本会重定向到 C:\Windows\sysWOW64\目录查找对应脚本。

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
C M I T

发件人: Wei Liang

发送时间: 2023 年 1 月 30 日 16:53

收件人: 许翔 <win10sup@sdicbc.com.cn>

抄送: ICBC_Notification <ICBC_Notification@cmgos.com>

主题: 回复: [案例号: CAS-08073-F5Y7B2] % |P2||ICBC|运行脚本报找不到指定路径 % 初次响应 CMIT:0001186

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:

用户反馈设备登录时 AdminScripts.vbs 脚本运行提示找不到指定路径, 需要协助分析。

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) 请您通过 CDUC 将此 vbs 脚本上传。
- 2) 请您运行 CMGELogCollectorV2.exe, 勾选**所有选项**, 点击**收集**获取对应的系统日志, 将生成的日志压缩包通过 CDUC 上传。



3) 请您使用 procmon.exe 抓取手动运行 AdminScripts.vbs 出现报错提示的 procmon 日志。

日志上传方法：

您可以登陆 <https://cdac.cmgos.com>，通过数据上传系统上传您所收集的日志信息。

用户名：icbcsupport

密码：icbcsupport

注意：添加文件，点击上传后，跳转到新的页面点击保存。

=====

在向 CMIT 提供日志和数据前，请阅读并接受邮件下方隐私声明。

隐私声明

为您提供本产品的相关技术支持及相关服务，您需要在同意本声明的前提下向神州网信提供为解决系统故障必要的数据和信息，包括但不限于与您相关的个人数据和隐私信息。通常情况下，我们仅需要如下数据以使我们的服务能够更好地满足您的需求：内存转储文件、注册表信息、组策略信息、事件日志、安装应用列表、驱动信息、网络日志或系统补丁等。

神州网信承诺将采取商业上可行及必要措施保护用户提供给神州网信的数据和信息，且仅在解决问题过程中使用。

神州网信保证不对外公开或向第三方提供、公开或共享您提供的数据和信息。

在以下情况下，神州网信对您的数据和信息的披露将不视为违约，具体包括：

- (1) 神州网信已获得您的明确授权;
- (2) 根据适用法律的要求, 神州网信负有披露义务的;
- (3) 司法机关或行政机关基于法定程序要求神州网信提供的;
- (4) 为维护社会公共利益及神州网信合法权益, 在合理范围内进行披露的。
- (5) 为了解决您的系统故障问题, 神州网信可能会与神州网信的分包商披露您提供的数据和信息。在此情况下, 第三方会承担与神州网信同等的隐私保护责任的, 神州网信会在合理范围内对您的信息进行披露。

如果您欲提供的数据和信息中包含对您重要的保密信息以及商业秘密, 在您向神州网信提供上述数据和信息前, 务必对上述数据和信息进行脱敏处理, 否则请不要提供该信息给神州网信。作为一家商业软件公司, 神州网信在商业可行的前提下, 已为用户的数据和信息保护做了极大的努力, 但是仍然不能保证现有的安全技术措施使您的数据和信息等不受任何形式的损失。您对上述情况充分知情, 且不会因此追究神州网信的法律责任。

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: 2023 年 1 月 30 日 16:12
收件人: 许翔 <win10sup@cdc.icbc.com.cn>
抄送: Wei Liang <weiliang@cmgos.com>
主题: [案例号: CAS-08073-F5Y7B2] % |P2|ICBC|运行脚本报找不到指定路径 % 初次响应
CMIT:0001186

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-08073-F5Y7B2 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”。