

许先生，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：**

V2020-L 版本 vbs 脚本输出文件位置错误

**案例进展：**

怀疑为执行脚本权限导致。由于出发方式不一致，问题日志发现为计划任务触发，正常日志手动触发，目前生产环境暂不复现问题，暂时归档案例。

---

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](mailto:jiawei@cmgos.com)

C&M Information Technologies Co., Ltd.  
11F, Block C North Building, Raycom InfoTech Park, Beijing  
mail: [Jiawei@cmgos.com](mailto:Jiawei@cmgos.com) | visit: [www.cmgos.com](http://www.cmgos.com)

---

**发件人:** Jia Wei  
**发送时间:** 2024 年 4 月 11 日 10:25  
**收件人:** ICBC 案例通知 <[win10sup@sdicbc.com.cn](mailto:win10sup@sdicbc.com.cn)>  
**抄送:** ICBC\_Notification <[ICBC\\_Notification@cmgos.com](mailto:ICBC_Notification@cmgos.com)>  
**主题:** 回复: [案例号: CAS-11161-M6Y0G6 ] % |P2|ICBC|工行用户反馈 V2020-L 版本 vbs 脚本安装失败问题 % 初次响应 CMIT:0001298

许先生，您好

根据之前电话沟通的结果，当前运行脚本输出位置正常的场景，是手动运行的。建议收集使用计划任务触发脚本运行的 Procmon 日志并反馈。

如果您有疑问可回复此邮件。

---

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](mailto:jiawei@cmgos.com)

C&M Information Technologies Co., Ltd.  
11F, Block C North Building, Raycom InfoTech Park, Beijing  
mail: [Jiawei@cmgos.com](mailto:Jiawei@cmgos.com) | visit: [www.cmgos.com](http://www.cmgos.com)

---

**发件人:** Jia Wei  
**发送时间:** 2024 年 4 月 3 日 17:51  
**收件人:** ICBC 案例通知 <[win10sup@sdicbc.com.cn](mailto:win10sup@sdicbc.com.cn)>  
**抄送:** ICBC\_Notification <[ICBC\\_Notification@cmgos.com](mailto:ICBC_Notification@cmgos.com)>  
**主题:** 回复: [案例号: CAS-11161-M6Y0G6 ] % |P2||ICBC|工行用户反馈 V2020-L 版本 vbs 脚本安装失败问题 % 初次响应 CMIT:0001298

许先生，您好

**问题定义:**

V2020-L 版本 vbs 脚本输出文件位置错误

**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。

### 问题分析:

- 1) 从脚本上看, 没有在代码中显式指定文件生成路径, 因此通常生成的文件将位于启动脚本所在目录下, 也就是 D:\ATAAgentMonitor
- 2) 基于上述理论, 当前问题的可能的原因之一是, 你运行这段代码的环境中, 当前工作目录是 C:\Windows\System32\。这种情况下, 生成的 Data.xml 文件会被保存在当前工作目录, 即 C:\Windows\System32\。
- 3) 我们看到一直在 C:\Windows\System32 目录下写 Data.xml 的 PID 为 3924 的进程。

Process Name	PID	Operation	Path
cscript.exe	3924	WriteFile	C:\Windows\System32\Data.xml
cscript.exe	3924	WriteFile	C:\Windows\System32\Data.xml
cscript.exe	3924	WriteFile	C:\Windows\System32\Data.xml
cscript.exe	3924	WriteFile	C:\Windows\System32\Data.xml

- 4) 这里对应的进程是 cscript.exe, 但是运行此进程的 User 是 NT AUTHORITY\SYSTEM。且对应的父进程是 svchost.exe(1652)

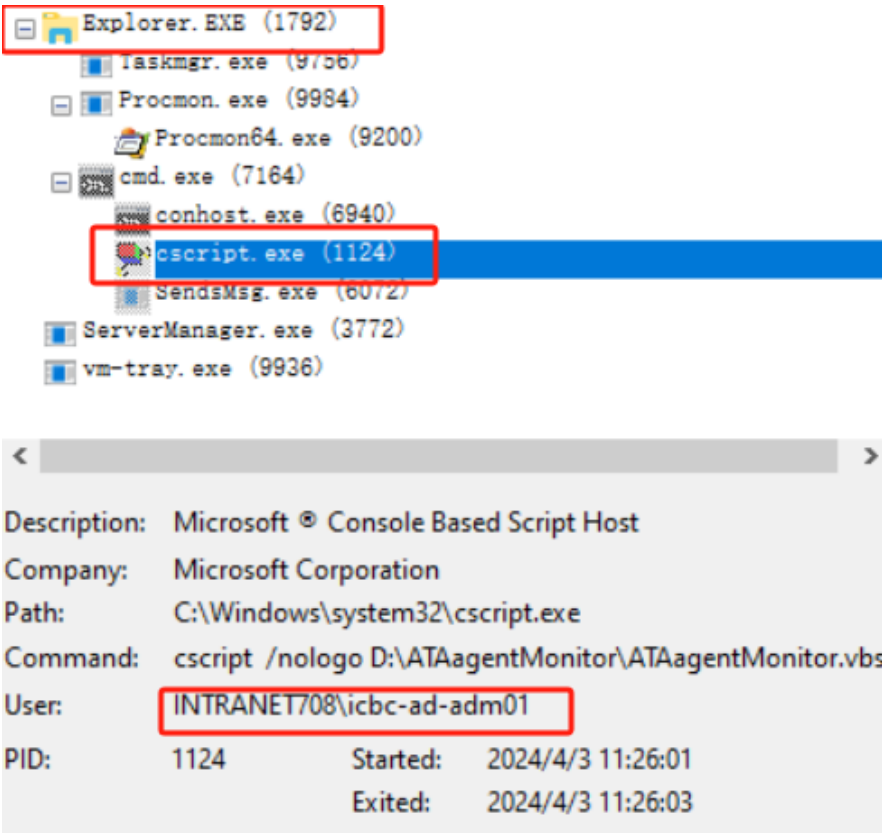
Task Manager process tree:

- svchost.exe (1652)
  - taskhostw.exe (6888)
  - taskhostw.exe (3968)
  - taskhostw.exe (2552)
  - cmd.exe (1012)
    - conhost.exe (10008)
    - cscript.exe (3924)**
    - taskhostw.exe (4744)
  - svchost.exe (2140)
  - svchost.exe (2168)
  - svchost.exe (2284)
  - svchost.exe (2388)

Properties window for cscript.exe:

- Description: Microsoft © Console Based Script Host
- Company: Microsoft Corporation
- Path: C:\Windows\system32\cscript.exe
- Command: cscript /nologo D:\ATAAgentMonitor\ATAAgentMonitor.vbs
- User: **NT AUTHORITY\SYSTEM**
- PID: 3924
- Started: 2024/4/2 13:05:00

5) 对比如下正常情况，此进程运行时的 User 对应的是当前登录用户，而父进程是 Explorer.EXE



- 6) 由于 SYSTEM 用户的运行环境就是 Windows\System32，所以解释了为什么会在此路径下生成 Data.xml
- 7) 而对应的命令行，应该是 Task Scheduler 服务，任务计划程序。所以建议排查是否有计划任务触发了脚本运行。

svchost.exe (1652)	Windows 服务主进程	C:\Windows\system32\svchost.exe
taskhostw.exe (6888)	Windows 任务的主机进程	C:\Windows\system32\taskhost.exe
taskhostw.exe (3968)	Windows 任务的主机进程	C:\Windows\system32\taskhost.exe
taskhostw.exe (2552)	Windows 任务的主机进程	C:\Windows\system32\taskhost.exe
cmd.exe (1012)	Windows 命令处理程序	C:\Windows\SYSTEM32\cmd.exe
conhost.exe (10008)	控制台窗口主进程	C:\Windows\system32\conhost.exe
cscript.exe (3924)	Microsoft © Console Based Script Host	C:\Windows\system32\cscript.exe
taskhostw.exe (4744)	Windows 任务的主机进程	C:\Windows\system32\taskhost.exe

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](mailto:jiawei@cmgos.com)

C&M Information Technologies Co., Ltd.  
11F, Block C North Building, Raycom InfoTech Park, Beijing  
mail: [Jiawei@cmgos.com](mailto:Jiawei@cmgos.com) | visit: [www.cmgos.com](http://www.cmgos.com)

---

**发件人:** Jia Wei <[jiawei@cmgos.com](mailto:jiawei@cmgos.com)>  
**发送时间:** 2024 年 4 月 3 日 17:04  
**收件人:** ICBC 案例通知 <[win10sup@sdicbc.com.cn](mailto:win10sup@sdicbc.com.cn)>  
**抄送:** Jia Wei <[jiawei@cmgos.com](mailto:jiawei@cmgos.com)>  
**主题:** [案例号: CAS-11161-M6Y0G6 ] % |P2|ICBC|工行用户反馈 V2020-L 版本 vbs 脚本安装失败问题 % 初次响应 CMIT:0001298

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-11161-M6Y0G6 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”。