许先生 您好:

感谢您的回复。

经过您的确认，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，如有其他问题，您可以随时联系我们。

案例总结：

问题定义：

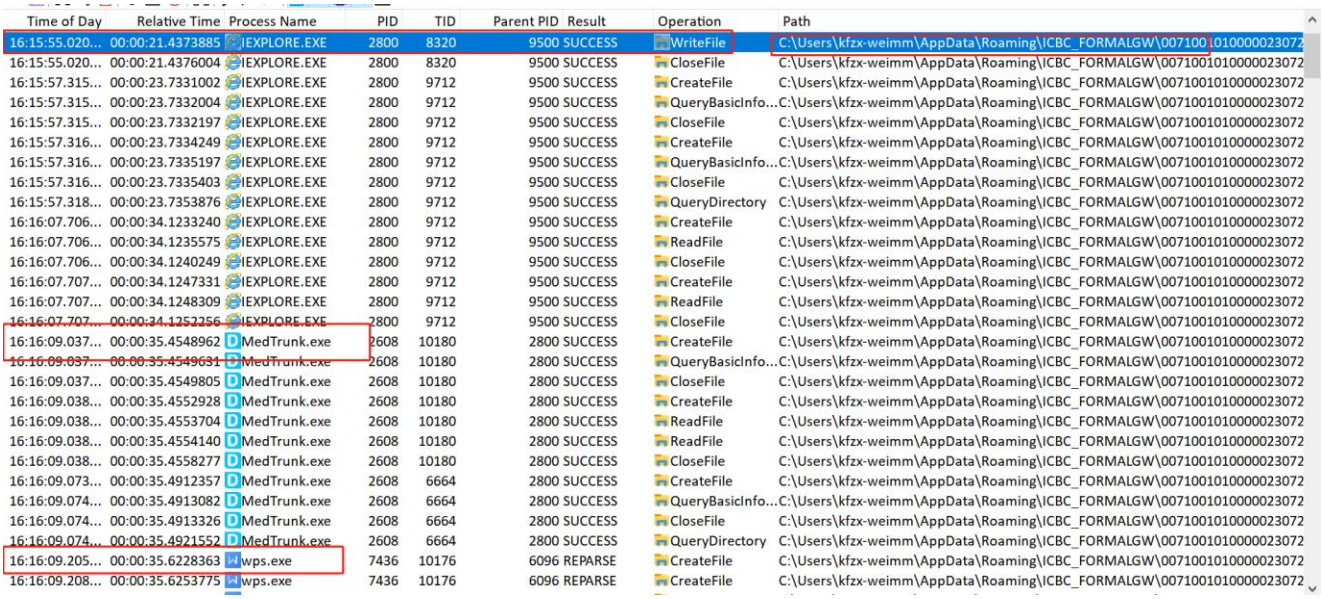
公文调用 wps 时效过长，目前 wps 厂商获取的日志分析和系统 ntdll.dll 组件信任有关，需要协助排查是否为系统自身行为阻止 IE 自动调用 wps。

问题总结：

用户确认案例可以关闭。

问题排查：

procmon 日志显示 IE 在 16:15:55 下载**“正文.doc”**文件后，直到 16:16:09 才调用 DSP 检测文件。最后 WPS 打开**“正文.doc”**文件。



Time of Day	Relative Time	Process Name	PID	TID	Parent PID	Result	Operation	Path
16:15:55.020...	00:00:21.4373885	IEXPLORE.EXE	2800	8320	9500	SUCCESS	WriteFile	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\007100101000002307
16:15:55.020...	00:00:21.4376004	IEXPLORE.EXE	2800	8320	9500	SUCCESS	CloseFile	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\007100101000002307
16:15:57.315...	00:00:23.7331002	IEXPLORE.EXE	2800	9712	9500	SUCCESS	CreateFile	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\007100101000002307
16:15:57.315...	00:00:23.7332004	IEXPLORE.EXE	2800	9712	9500	SUCCESS	QueryBasicInfo...	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\007100101000002307
16:15:57.315...	00:00:23.7332197	IEXPLORE.EXE	2800	9712	9500	SUCCESS	CloseFile	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\007100101000002307
16:15:57.316...	00:00:23.7334249	IEXPLORE.EXE	2800	9712	9500	SUCCESS	CreateFile	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\007100101000002307
16:15:57.316...	00:00:23.7335197	IEXPLORE.EXE	2800	9712	9500	SUCCESS	QueryBasicInfo...	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\007100101000002307
16:15:57.316...	00:00:23.7335403	IEXPLORE.EXE	2800	9712	9500	SUCCESS	CloseFile	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\007100101000002307
16:15:57.318...	00:00:23.7353876	IEXPLORE.EXE	2800	9712	9500	SUCCESS	QueryDirectory	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\007100101000002307
16:16:07.706...	00:00:34.1233240	IEXPLORE.EXE	2800	9712	9500	SUCCESS	CreateFile	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\007100101000002307
16:16:07.706...	00:00:34.1235575	IEXPLORE.EXE	2800	9712	9500	SUCCESS	ReadFile	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\007100101000002307
16:16:07.706...	00:00:34.1240249	IEXPLORE.EXE	2800	9712	9500	SUCCESS	CloseFile	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\007100101000002307
16:16:07.707...	00:00:34.1247331	IEXPLORE.EXE	2800	9712	9500	SUCCESS	CreateFile	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\007100101000002307
16:16:07.707...	00:00:34.1248309	IEXPLORE.EXE	2800	9712	9500	SUCCESS	ReadFile	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\007100101000002307
16:16:07.707...	00:00:34.1252256	IEXPLORE.EXE	2800	9712	9500	SUCCESS	CloseFile	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\007100101000002307
16:16:09.037...	00:00:35.4548962	MedTrunk.exe	2608	10180	2800	SUCCESS	CreateFile	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\007100101000002307
16:16:09.037...	00:00:35.4549631	MedTrunk.exe	2608	10180	2800	SUCCESS	QueryBasicInfo...	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\007100101000002307
16:16:09.037...	00:00:35.4549805	MedTrunk.exe	2608	10180	2800	SUCCESS	CloseFile	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\007100101000002307
16:16:09.038...	00:00:35.4552928	MedTrunk.exe	2608	10180	2800	SUCCESS	CreateFile	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\007100101000002307
16:16:09.038...	00:00:35.4553704	MedTrunk.exe	2608	10180	2800	SUCCESS	ReadFile	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\007100101000002307
16:16:09.038...	00:00:35.4554140	MedTrunk.exe	2608	10180	2800	SUCCESS	ReadFile	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\007100101000002307
16:16:09.038...	00:00:35.4558277	MedTrunk.exe	2608	10180	2800	SUCCESS	CloseFile	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\007100101000002307
16:16:09.073...	00:00:35.4912357	MedTrunk.exe	2608	6664	2800	SUCCESS	CreateFile	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\007100101000002307
16:16:09.074...	00:00:35.4913082	MedTrunk.exe	2608	6664	2800	SUCCESS	QueryBasicInfo...	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\007100101000002307
16:16:09.074...	00:00:35.4913326	MedTrunk.exe	2608	6664	2800	SUCCESS	CloseFile	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\007100101000002307
16:16:09.074...	00:00:35.4921552	MedTrunk.exe	2608	6664	2800	SUCCESS	QueryDirectory	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\007100101000002307
16:16:09.205...	00:00:35.6228363	wps.exe	7436	10176	6096	REPARSE	CreateFile	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\007100101000002307
16:16:09.208...	00:00:35.6253775	wps.exe	7436	10176	6096	REPARSE	CreateFile	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\007100101000002307

时间主要花费在下载“正文.doc”后到调用 dsp 的过程。需要确认 IE 访问并下载**“正文.doc”**文件是哪一个插件完成的，排查其行为逻辑。

下载的 doc 文件所在位置：

C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\00710010100000230727144437615A07\正文.doc

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: win10 技术支持 <win10sup@sdc.icbc.com.cn>
发送时间: 2023 年 8 月 3 日 15:52
收件人: Wei Liang <weiliang@cmgos.com>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复：【外来邮件，注意核实】回复: [案例号：CAS-09513-T6V3V0] % |P2|ICBC|工行公文调用 wps 时效异常 % 初次响应 CMIT:0001450

wps 时效问题，请关单。

☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆

中国工商银行软件开发中心（珠海）
许 翔
系统一部
电话：17606669571

☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆

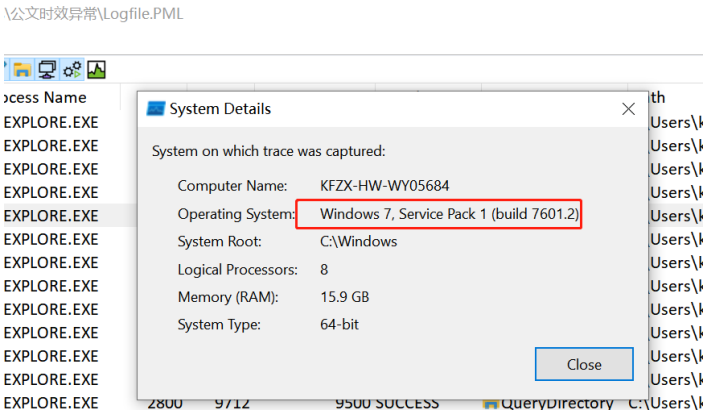
-----原始邮件-----

发件人: "Wei Liang" <weiliang@cmgos.com>
发送时间: 2023-08-01 11:44:42
收件人: "win10 技术支持" <win10 技术支持.软件开发中心系统一部@工商银行.icbc>
抄送: "ICBC_Notification" <icbc_notification@cmgos.com>
主题: 【外来邮件，注意核实】回复: [案例号: CAS-09513-T6V3V0] % |P2|ICBC|工行公文调用 wps 时效异常 % 初次响应 CMIT:0001450

许先生 您好:

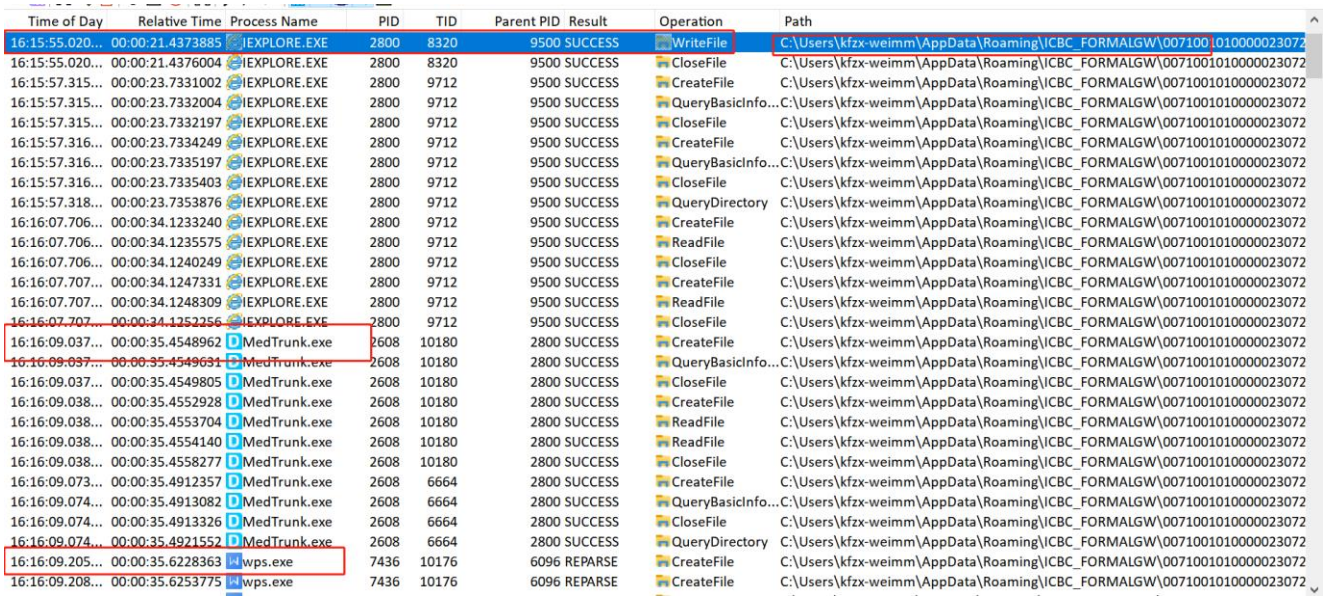
感谢您的电话接听。

您提供的 procmon 日志显示这个日志是在 Windows 7 上收取的日志。



麻烦您在神州网信政府版系统上复现问题并收集对应的 procmon 日志。

当前的 procmon 日志显示 IE 在 16:15:55 下载**“正文.doc”**文件后，直到 16:16:09 才调用 DSP 检测文件。最后 WPS 打开**“正文.doc”**文件。



Time of Day	Relative Time	Process Name	PID	TID	Parent PID	Result	Operation	Path
16:15:55.020...	00:00:21.4373885	IEXPLORE.EXE	2800	8320	9500	SUCCESS	WriteFile	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\007100[illegible]010000023072
16:15:55.020...	00:00:21.4376004	IEXPLORE.EXE	2800	8320	9500	SUCCESS	CloseFile	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\0071001010000023072
16:15:57.315...	00:00:23.7331002	IEXPLORE.EXE	2800	9712	9500	SUCCESS	CreateFile	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\0071001010000023072
16:15:57.315...	00:00:23.7332004	IEXPLORE.EXE	2800	9712	9500	SUCCESS	QueryBasicInfo...	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\0071001010000023072
16:15:57.315...	00:00:23.7332197	IEXPLORE.EXE	2800	9712	9500	SUCCESS	CloseFile	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\0071001010000023072
16:15:57.316...	00:00:23.7334249	IEXPLORE.EXE	2800	9712	9500	SUCCESS	CreateFile	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\0071001010000023072
16:15:57.316...	00:00:23.7335197	IEXPLORE.EXE	2800	9712	9500	SUCCESS	QueryBasicInfo...	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\0071001010000023072
16:15:57.316...	00:00:23.7335403	IEXPLORE.EXE	2800	9712	9500	SUCCESS	CloseFile	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\0071001010000023072
16:15:57.318...	00:00:23.7353876	IEXPLORE.EXE	2800	9712	9500	SUCCESS	QueryDirectory	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\0071001010000023072
16:16:07.706...	00:00:34.1233240	IEXPLORE.EXE	2800	9712	9500	SUCCESS	CreateFile	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\0071001010000023072
16:16:07.706...	00:00:34.1235575	IEXPLORE.EXE	2800	9712	9500	SUCCESS	ReadFile	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\0071001010000023072
16:16:07.706...	00:00:34.1240249	IEXPLORE.EXE	2800	9712	9500	SUCCESS	CloseFile	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\0071001010000023072
16:16:07.707...	00:00:34.1247331	IEXPLORE.EXE	2800	9712	9500	SUCCESS	CreateFile	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\0071001010000023072
16:16:07.707...	00:00:34.1248309	IEXPLORE.EXE	2800	9712	9500	SUCCESS	ReadFile	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\0071001010000023072
16:16:07.707...	00:00:34.1252256	IEXPLORE.EXE	2800	9712	9500	SUCCESS	CloseFile	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\0071001010000023072
16:16:09.037...	00:00:35.4548962	MedTrunk.exe	2608	10180	2800	SUCCESS	CreateFile	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\0071001010000023072
16:16:09.037...	00:00:35.4549631	MedTrunk.exe	2608	10180	2800	SUCCESS	QueryBasicInfo...	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\0071001010000023072
16:16:09.037...	00:00:35.4549805	MedTrunk.exe	2608	10180	2800	SUCCESS	CloseFile	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\0071001010000023072
16:16:09.038...	00:00:35.4552928	MedTrunk.exe	2608	10180	2800	SUCCESS	CreateFile	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\0071001010000023072
16:16:09.038...	00:00:35.4553704	MedTrunk.exe	2608	10180	2800	SUCCESS	ReadFile	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\0071001010000023072
16:16:09.038...	00:00:35.4554140	MedTrunk.exe	2608	10180	2800	SUCCESS	ReadFile	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\0071001010000023072
16:16:09.038...	00:00:35.4558277	MedTrunk.exe	2608	10180	2800	SUCCESS	CloseFile	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\0071001010000023072
16:16:09.073...	00:00:35.4912357	MedTrunk.exe	2608	6664	2800	SUCCESS	CreateFile	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\0071001010000023072
16:16:09.074...	00:00:35.4913082	MedTrunk.exe	2608	6664	2800	SUCCESS	QueryBasicInfo...	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\0071001010000023072
16:16:09.074...	00:00:35.4913326	MedTrunk.exe	2608	6664	2800	SUCCESS	CloseFile	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\0071001010000023072
16:16:09.074...	00:00:35.4921552	MedTrunk.exe	2608	6664	2800	SUCCESS	QueryDirectory	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\0071001010000023072
16:16:09.205...	00:00:35.6228363	wps.exe	7436	10176	6096	REPARSE	CreateFile	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\0071001010000023072
16:16:09.208...	00:00:35.6253775	wps.exe	7436	10176	6096	REPARSE	CreateFile	C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\0071001010000023072

需要请您确认 IE 访问并下载**“正文.doc”**文件是哪一个插件完成的，它是否需要对**“正文.doc”**文件做相关的校验检测。

下载的 doc 文件所在位置：

C:\Users\kfzx-weimm\AppData\Roaming\ICBC_FORMALGW\00710010100000230727144437615A07\正文.doc

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 7 月 31 日 18:19
收件人: 许翔 <win10sup@sdc.icbc.com.cn>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>

主题: 回复: [案例号: CAS-09513-T6V3V0] % |P2|ICBC|工行公文调用 wps 时效异常 % 初次响应 CMIT:0001450

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:

公文调用 wps 时效过长，目前 wps 厂商获取的日志分析和系统 ntdll.dll 组件信任有关，需要协助排查是否为系统自身行为阻止 IE 自动调用 wps。

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。

我先查看您提供的 procmon 日志，有任何进展会及时与您联系。也麻烦您帮忙准备可以复现问题的测试环境，用于后续相关的日志收集和测试操作。

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 7 月 31 日 17:14
收件人: 许翔 <win10sup@sdc.icbc.com.cn>
抄送: Wei Liang <weiliang@cmgos.com>
主题: [案例号: CAS-09513-T6V3V0] % |P2|ICBC|工行公文调用 wps 时效异常 % 初次响应 CMIT:0001450

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-09513-T6V3V0 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”。