

边先生，您好：

如刚才电话沟通，经您的确认，目前蓝屏问题已解决，此 case 将做关闭处理，以下为案例总结，请您：

Case No: CAS-08433-X3V6G7

问题描述：

=====

用户反馈蓝屏问题。

问题分析：

=====

经 dump 分析，用户日志中反映的蓝屏问题为驱动程序尝试写入只读内存段导致。请用户按之前邮件进行三方驱动的排查，并后续观察。

问题总结：

=====

经用户确认，目前问题已解决，该问题做关闭处理。

以上为此问题的案例总结，如有任何问题，可随时与我们联系，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: 2023 年 3 月 13 日 14:17

收件人: '1206596688@qq.com' <1206596688@qq.com>

抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>

主题: 回复: [案例号: CAS-08433-X3V6G7] %TAM 反馈中信建投客户系统蓝屏问题% 案例重新分配 CMIT:0001887

边先生, 您好:

根据您上传的 dump 及系统日志, 有如下发现供您参考:

首先, 从您提供的系统日志来看, 当前电脑存在多次蓝屏的情况, 且蓝屏原因均不相同。列举以下部分信息:

20230310 事件数: 10,725				
已筛选: 日志: file:///C:/Users/liqi/Downloads/20230310.evtx; 来源: Microsoft-Windows-WER-SystemErrorReporting; 事件数: 8				
级别	日期和时间	来源	事件 ID	任务类别
错误	2023/3/10 13:31:58	BugCheck	1001	无
错误	2023/3/10 8:46:38	BugCheck	1001	无
错误	2023/3/9 18:50:34	BugCheck	1001	无
错误	2023/3/9 16:09:03	BugCheck	1001	无
错误	2023/3/9 13:05:19	BugCheck	1001	无
错误	2023/3/6 8:22:23	BugCheck	1001	无
错误	2023/3/1 17:02:23	BugCheck	1001	无
错误	2023/3/1 8:50:48	BugCheck	1001	无

事件 1001, BugCheck	
常规	详细信息
计算机已经从检测错误后重新启动。检测错误: 0x0000001a (0x0000000000041792, 0xfffff9bffc322580, 0xfffff0000000000000, 0x0000000000000000), 已将转储的数据保存在: C:\Windows\MEMORY.DMP, 报告 ID: 758e81d0-9592-4563-8137-88b4ac0314b1。	

Bugcheck 0xbe: ATTEMPTED_WRITE_TO_READONLY_MEMORY bug 检查的值为

0x000000BE。如果驱动程序尝试写入只读内存段, 则会发出此问题。

Bugcheck 0x1a: MEMORY_MANAGEMENT bug 检查的值为 0x0000001A。错误检查指示发生了严重的内存管理错误。

Bugcheck 0xc2: BAD_POOL_CALLER bug 检查的值为 0x000000C2。这表示当前线程正在发出错误的池请求。

Bugcheck 0x7e: SYSTEM_THREAD_EXCEPTION_NOT_HANDLED bug 检查的值为 0x0000007E。此 bug 检查指示系统线程生成了错误处理程序未捕获的异常。

还有其他的 bugcheck 信息，此处不一一列出。关于您此次上传的 dump 日志记录的为 3/10 13:31 发生的 bugcheck 0xbe 的蓝屏问题。

ATTEMPTED_WRITE_TO_READONLY_MEMORY (be)

An attempt was made to write to readonly memory. The guilty driver is on the stack trace (and is typically the current instruction pointer).

When possible, the guilty driver's name (Unicode string) is printed on the BugCheck screen and saved in KiBugCheckDriver.

Arguments:

Arg1: fffffec500007038, Virtual address for the attempted write.

Arg2: 8a00000004000021, PTE contents.

Arg3: fffff582b04ea8d0, (reserved)

Arg4: 000000000000000b, (reserved)

从 call stack 可以看到该问题是由于会话子进程管理的进程 smss 试图写入只读内存时发生的蓝屏问题。

fffff582`b04ea628 fffff800`73436f8d : 00000000`000000be fffffec5`00007038

8a000000`04000021 fffff582`b04ea8d0 : nt!KeBugCheckEx

fffff582`b04ea630 fffff800`73242250 : fffff582`00000000 00000000`00000003

fffff582`b04ea950 00000000`00000000 : nt!MiSystemFault+0x1d6d0d

fffff582`b04ea730 fffff800`73409cd8 : fffffa208`fb513870 fffffb808`95ed2010 fffffa208`00000000

fffffb808`812ae040 : nt!MmAccessFault+0x400

fffff582`b04ea8d0 fffff800`732cc9f1 : 00000000`000001c0 fffff800`732ca537

00000000`00000000 fffff800`73c4edc0 : nt!KiPageFault+0x358

fffff582`b04eaa60 fffff800`732ca537 : 00000000`00000000 fffff800`73c4edc0 fffff901`af787370

00000000`00000010 : nt!RtlInterlockedSetClearRunEx+0x71

fffff582`b04eaa70 fffff800`7326caef : 00000000`00000010 fffff582`00000000

00000000`00000000 00000000`00000000 : nt!MiReservePtes+0x297

fffff582`b04eab40 fffff800`736510e0 : fffff901`af7870c0 fffffb808`882dc201 fffff582`b04eae60

fffff582`b04eadc8 : nt!MiInsertInSystemSpace+0x1ef

fffff582`b04eacc0 fffff800`736ef381 : 00000000`00000000 fffff582`b04eade9
fffff582`b04eb0e0 00000000`c0000001 : nt!MiMapViewInSystemSpace+0xc0
fffff582`b04ead20 fffff800`736ef31a : fffffb808`81293da0 fffff800`733fedb0
00000000`00000010 00000000`00040082 : nt!MmMapViewInSessionSpaceEx+0x51
fffff582`b04ead70 fffffedc`2ce0b60d : 00000000`00000000 fffffedc`2cb12f47
00000000`00000030 00000000`00000000 : nt!MmMapViewInSessionSpace+0x1a
fffff582`b04eadb0 fffffedc`2cc9581d : ffffffff`800038a0 ffffa208`fb513870 00000000`00000030
00000000`00000000 : win32kfull!InitializeWin32CrossSessionGlobals+0x10d
fffff582`b04eae50 fffffedc`2d641298 : 00000000`c0000002 00000000`00000000
fffff582`b04eb0e0 fffff582`b04eb0e0 : win32kbase!Win32kBaseDriverEntry+0x21d
fffff582`b04eb040 fffffedc`2d641450 : 00000000`00000000 fffff582`b04eb7b8
fffff582`b04eb0b8 00000000`00000018 : win32k!DriverEntry+0x70
fffff582`b04eb090 fffff800`73786015 : fffffedc`2d5b0000 fffff582`b04eb100
00000005`00000001 fffff800`00000001 : win32k!GsDriverEntry+0x20
fffff582`b04eb0c0 fffff800`735d824c : 00000000`00000000 fffffedc`2d5b0100
00000000`00000000 fffff582`b04eb400 : nt!ExpInitializeSessionDriver+0x39
fffff582`b04eb240 fffff800`7340d9f8 : ffffa209`12d397c0 fffff582`b04eb710
00000000`00000001 fffff800`73628601 : nt!NtSetSystemInformation+0x74c
fffff582`b04eb5d0 fffff800`733fedb0 : fffff800`735d81a4 00000000`00000000
00000000`00000000 00000000`00000000 : nt!KiSystemServiceCopyEnd+0x28
fffff582`b04eb768 fffff800`735d81a4 : 00000000`00000000 00000000`00000000
00000000`00000000 00000000`00000000 : nt!KiServiceLinkage
fffff582`b04eb770 fffff800`7340d9f8 : fffffb808`960a1080 00000000`00000003
00000000`00000000 00000028`c5def918 : nt!NtSetSystemInformation+0x6a4
fffff582`b04ebb00 00007ff8`4ad905f4 : 00007ff7`10844124 00000000`00000002
00000028`c5def8e0 00000000`00000010 : nt!KiSystemServiceCopyEnd+0x28
00000028`c5def888 00007ff7`10844124 : 00000000`00000002 00000028`c5def8e0
00000000`00000010 00007ff7`10858cc0 : ntdll!NtSetSystemInformation+0x14

```
00000028`c5def890 00007ff7`10844046 : 00000000`00000002 00000163`94e04840
00000163`94e04280 00000000`ffffff : smss!SmscpLoadSubSystemsForMuSession+0xa4
00000028`c5def910 00007ff7`10841972 : 00000000`00000001 00000000`00000000
00000000`00000000 ffffffff`fd050f80 : smss!SmscMain+0xfa
00000028`c5def950 00007ff7`108417ea : 00000000`000000e8 00000000`000001aa
00000000`00000000 00000000`00000000 : smss!wmain+0x132
00000028`c5defaa0 00007ff7`10841506 : 00000000`00000005 00000000`00000000
00000163`94e04280 00000000`00000000 :
smss!NtProcessStartupW_AfterSecurityCookieInitialized+0x2da
00000028`c5defb20 00007ff8`4ad426af : 00000000`00000000 00000000`00000000
00000000`00000000 00000000`00000000 : smss!NtProcessStartupW+0x16
00000028`c5defb50 00000000`00000000 : 00000000`00000000 00000000`00000000
00000000`00000000 00000000`00000000 : ntdll!RtlUserThreadStart+0x2f
```

问题内存地址无法获取到有效信息，故而出现错误。

```
4: kd> dd 8a00000004000021
```

```
8a000000`04000021 ???????? ???????? ???????? ????????
8a000000`04000031 ???????? ???????? ???????? ????????
8a000000`04000041 ???????? ???????? ???????? ????????
8a000000`04000051 ???????? ???????? ???????? ????????
8a000000`04000061 ???????? ???????? ???????? ????????
8a000000`04000071 ???????? ???????? ???????? ????????
8a000000`04000081 ???????? ???????? ???????? ????????
8a000000`04000091 ???????? ???????? ???????? ????????

```

进一步查看当前运行进程情况，可以看到系统进程正在等待从硬盘交换内存数据的行为。

Process	PID	Thread	Id	Pri	Base Pri	Next CPU	CSwitches	User	Kernel	State	Time	Reason
Idle	0	fffff80073d27a00	0	0	0	0	942171	0	1h:54:39.047	Running	140ms	Executi
Idle	0	ffffc901a6b8b440	0	0	0	1	633843	0	1h:57:47.078	Running	5s.015	Executi
Idle	0	ffffc901a6c0b440	0	0	0	2	955637	0	1h:50:57.438	Running	296ms	Executi
Idle	0	ffffc901a6ccb440	0	0	0	3	628928	0	1h:57:33.078	Running	2s.421	Executi
smss.exe	a48	fffffb808960a1080	2c54	9	8	4	3	0	0	Running	0	Executi
Idle	0	ffffc901a6df7440	0	0	0	5	625550	0	1h:57:30.063	Running	6s.028	Executi
System	4	fffffb80896159040	2fd8	12	12	6	1452	0	344ms	Running	0	WrProce
Idle	0	ffffc901a6f6b440	0	0	0	7	595340	0	1h:57:30.797	Running	203ms	Executi
Idle	0	ffffc901a704b440	0	0	0	8	1050902	0	1h:54:57.141	Running	1s.265	Executi
Idle	0	ffffc901a710b440	0	0	0	9	611395	0	1h:57:56.969	Running	7s.578	Executi
Idle	0	ffffc901a71cb440	0	0	0	10	1392087	0	1h:50:10.094	Running	250ms	Executi
Idle	0	ffffc901a7284440	0	0	0	11	682973	0	1h:56:23.453	Running	1s.859	Executi
Idle	0	ffffc901a733b440	0	0	0	12	988968	0	1h:56:38.641	Running	750ms	Executi
Idle	0	ffffc901a73eb440	0	0	0	13	548400	0	1h:57:27.531	Running	25s.453	Executi
Idle	0	ffffc901a74a7440	0	0	0	14	789040	0	1h:56:26.359	Running	0	Executi
Idle	0	ffffc901a755f440	0	0	0	15	567297	0	1h:55:46.344	Running	421ms	Executi

Count: 16 | [Show Unique Stacks](#)

由于当前 dump 并不能记录问题内存地址的生成过程，因此怀疑 smss 进程收到 system 进程申请从硬盘交换内存的指令后进行会话切换的动作，进而造成的访问只读内存地址时蓝屏。那么我们看下 system 进程正在做些什么呢？

```

4: kd> !mex.t`fffffb80896159040
Unable to load image \SystemRoot\system32\Drivers\SfUemFesfIsolate.sys, Win32 error 0n2
Process
System (fffffb808812ae040) AttachedProcess Thread
Agent.exe (fffffb8088f948080) fffffb80896159040 (E|K|W|R|V) 4.2fd8 0
Priority:
Current Base Decrement ForegroundBoost IO Page
12 12 0 0 0 5

```

```

# Child-SP Return Call Site
0 fffff582b79127c0 fffff8007624871b SfUemFesfIsolate+0x1b54f
1 fffff582b7912850 fffff80076248e5b FLTMRGR!FltpGetNormalizedFileNameWorker+0x18b
2 fffff582b79128d0 fffff8007621362f FLTMRGR!FltpCreateFileNameInformation+0x2eb
3 fffff582b7912950 fffff8007624828a FLTMRGR!FltpGetFileNameInformation+0x6ef
4 fffff582b7912a00 fffff8007a238f93 FLTMRGR!FltpGetFileNameInformationUnsafe+0x8a
5 fffff582b7912a80 fffff8007624871b SfUemIsoSpace+0x38f93
6 fffff582b7912ad0 fffff80076248e5b FLTMRGR!FltpGetNormalizedFileNameWorker+0x18b
7 fffff582b7912b50 fffff8007621362f FLTMRGR!FltpCreateFileNameInformation+0x2eb
8 fffff582b7912bd0 fffff8007624828a FLTMRGR!FltpGetFileNameInformation+0x6ef
9 fffff582b7912c80 fffff800762474d2 FLTMRGR!FltpGetFileNameInformationUnsafe+0x8a
a fffff582b7912d00 fffff80073682f33 FLTMRGR!FltpMgrFsRtlGetFileNameInformation+0x62
b fffff582b7912d40 fffff80073793d69 nt!EtwpEnumerateAddressSpace+0x233
c fffff582b7912ef0 fffff80073695013 nt!EtwpProcessEnumCallback+0x1f9
d fffff582b7912f90 fffff80073793b18 nt!PsEnumProcesses+0x37
e fffff582b7912fc0 fffff80073793904 nt!EtwpProcessThreadImageRundown+0xc0
f fffff582b7913050 fffff8007379374d nt!EtwpKernelTraceRundown+0x98
10 fffff582b79130c0 fffff800737934ff nt!EtwpUpdateGroupMasks+0x22d
11 fffff582b7913180 fffff800737191e5 nt!EtwpUpdateLoggerGroupMasks+0x73
12 fffff582b79131e0 fffff800737acaf1 nt!EtwpStartLogger+0xad9
13 fffff582b7913350 fffff800737abe59 nt!EtwStartAutoLogger+0x9f5
14 fffff582b7913b00 fffff800737aceaa4 nt!PerfDiagpStartPerfDiagLogger+0xdd
15 fffff582b7913b30 fffff8007325b3d5 nt!PerfDiagpProxyWorker+0x124
16 fffff582b7913b70 fffff800733030e5 nt!ExpWorkerThread+0x105
17 fffff582b7913c10 fffff80073402e08 nt!PspSystemThreadStartup+0x55
18 fffff582b7913c60 0000000000000000 nt!KiStartSystemThread+0x28

```

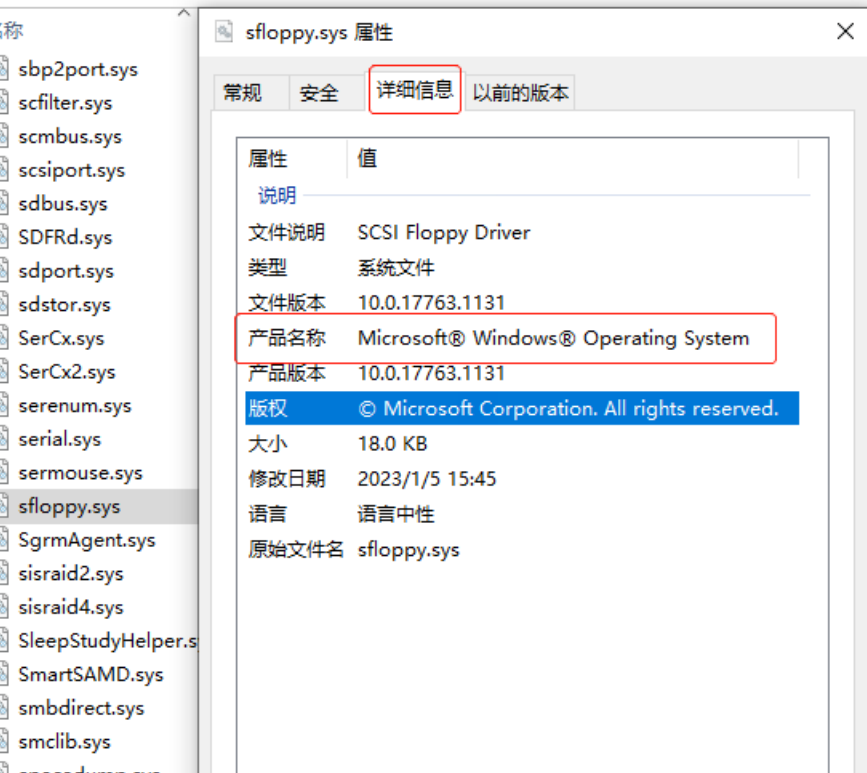
```

0: kd> !mex.p 0xfffffb8088f948080
Name Address Ses PID Parent PEB Create Time
Agent.exe fffffb8088f948080 (E|K|Q) 0 17e4 (0n6116) 2c4 (0n708) 000000401262d000 03/10/2023 08:46:41.191 L
Command Line: "C:\Program Files\DataCloak_DCube\Bin\DCubeAgent\Agent.exe"

```

我在我的电脑上并没有找到 c:\windows\system32\drivers\SfUemIsoSpace.sys 这个文件，该文件应属于第三方驱动，您可以通过以下方式确认：

右键单击该文件，选择属性，查看详细信息，如非 Microsoft 则为第三方驱动，您可以将其重命名或剪切至其他路径。



另外 system 进程正在执行的 command line 为 C:\Program Files\DataCloak_DCube\Bin\DCubeAgent\Agent.exe，请确认该文件是否可以暂时删除。

另结合您其他的蓝屏记录，多为内存相关错误，请尝试以下操作：


执行 cmd 命令：mdsched


管理员: C:\WINDOWS\system32\cmd.exe

Microsoft Windows [版本 10.0.22621.1265]
(c) Microsoft Corporation。保留所有权利。

C:\Users\liqi>mdsched

C:\Users\liqi>

 Windows 内存诊断

 **检查计算机的内存问题**

内存问题可使计算机丢失信息或停止工作。

[→ 立即重新启动并检查问题\(推荐\)](#)
请在重新启动前保存工作并关闭任何程序。

[→ 下次启动计算机时检查问题](#)

Windows 内存诊断工具

Windows 正在检查内存问题...
这可能需要几分钟的时间。

运行测试通过 1 个 (共 2)：06% 完成
总体测试状态：03% 完成



状态：
尚未检测到问题。

虽然测试有时看起来处于非活动状态，但是它仍在运行。请等待测试完成...

Windows 将自动重新启动计算机。在你登录后将再次显示测试结果。

检查内存是否存在问题。具体信息可在 Windows Logs > System > MemoryDiagnostics-Results 中查看。



2, 对于内存错误问题的蓝屏问题, 通常排查中会出现一种情况, 即当前访问的内存地址 (读或写) 是系统之前创建的, 由于 dump 是内存片段信息, 因此无法追溯该内存地址的创建过程, 通常这种情况下, 我们需要收集 TTT 来做动态跟踪, 但开启 TTT 会导致性能下降, 鉴于您当前的这个问题并不是必现场景, 可以继续观察, 如再出现类似蓝屏问题, 及时与我们联系, 进行后续处理。

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 3 月 9 日 17:39

收件人: '1206596688@qq.com' <1206596688@qq.com>

抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>

主题: 回复: [案例号: CAS-08433-X3V6G7] %TAM 反馈中信建投客户系统蓝屏问题% 案例重新分配 CMIT:0001887

边先生, 您好:

根据您的需求, 我谨以此封邮件阐述我们双方针对这个问题所涉及范围界定:

问题定义:

用户反馈蓝屏问题。

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。

下一步动作:

请您将收集的 **dump 日志** 按以下方法上传至 CDUC。

日志上传方法:

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

用户名: zxjtbian01

密码: zxjtbian01

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

为向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。

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
C M I T

发件人: CRM 管理员 <crmadmin@cmgos.com>

发送时间: 2023 年 3 月 9 日 17:28

收件人: Li Qi <liqi@cmgos.com>

主题: [案例号:CAS-08433-X3V6G7] %TAM 反馈中信建投客户系统蓝屏问题% 案例重新分配
CMIT:0001887

Hi 李琦

一个案例已被重新分配给您, 请及时处理。

案例号码: [CAS-08433-X3V6G7](#)

案例等级: 免费

案例描述: support 邮箱收到 TAM 李延晶发来邮件, 反馈中信建投客户系统蓝屏问题, 申请开 Case 处理, 已提供日志文件, 请协助分析。

邮件内容如下, 原邮件请见注释。

=====

附件为系统日志信息。

Best Regards

Jacky Li

李延晶

发件人: Li Yanjing

发送时间: 2023 年 3 月 9 日 17:10

收件人: Support

抄送: Liu Jian

主题: 回复: 中信建投客户反馈蓝屏问题

更正一下内部联系人信息。

Best Regards

Jacky Li

李延晶

发件人: Li Yanjing
发送时间: 2023 年 3 月 9 日 17:08
收件人: Support
抄送: Liu Jian
主题: 中信建投客户反馈蓝屏问题

Hi support team

中信建投客户反馈蓝屏问题 dump 日志已收集但需要上传路径, 请开案例协助支持, 今天需要联系用户给 cduc 上传路径, 谢谢!

合同: CMIT 服务
等级: 普通案例
客户联系人: 边雷阳
联系方式: 13126619225 / 1206596688@qq.com
TAM 联系人: 刘健/李延晶

Best Regards,
Jacky Li (李延晶)
Mobile: + 86 13552345377| Email: liyj@cmgos.com
创建人: 吴闫杰
创建时间: 2023/3/9 17:23