洪先生 您好:

根据刚才的电话沟通，我将暂时归档此案例。

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：

总行 Windows 10 神州网信政府版 V0-H 不定时出现蓝屏。

问题总结：

从 dump 中分析与亚信安全软件有关，用户升级亚信安全软件查看后续运行情况。

问题分析：

从上传的 dump 中分析蓝屏的原因，查看 callstack 与亚信安全的相关模块 VSApiNt 和 TmXPFlt 有关，建议升级亚信安全软件。

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

神州网信
CMIT

发件人: Wei Liang
发送时间: 2021 年 9 月 9 日 15:18

收 件 人： ' 吴 毓 杰 ' <win10sup@sdc.icbc.com.cn>; 'hongbo@icbc.com.cn' <hongbo@icbc.com.cn>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: [案例号: CAS-04716-C3F2K9] % |P3|ICBC|总行 win10 神州网信政府版电脑蓝屏 % 初次响应 CMIT:0001032

洪先生 您好:

感谢电话沟通，了解到您这边已经在 V0-H 系统上升级亚信安全软件。

升级亚信安全软件后，请观察一段时间是否还会出现蓝屏现象。

针对当前案件如果有需要我们帮助的地方, 欢迎随时联系我们。

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: 2021 年 9 月 8 日 16:46
收 件 人： ' 吴 毓 杰 ' <win10sup@sdc.icbc.com.cn>; 'hongbo@icbc.com.cn' <hongbo@icbc.com.cn>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: [案例号: CAS-04716-C3F2K9] % |P3|ICBC|总行 win10 神州网信政府版电脑蓝屏 % 初次响应 CMIT:0001032

洪先生 您好:

感谢电话沟通，这两次的 dump 分析如下:

第一次 dump，BugCheck：0x1a，提示是由于 VSApiNt 模块导致系统进程蓝屏。

```
*******************************************************************************
*                                                                             *
*                        Bugcheck Analysis                                    *
*                                                                             *
*******************************************************************************

MEMORY_MANAGEMENT (1a)
    # Any other values for parameter 1 must be individually examined.
Arguments:
Arg1: 0000000000041792, A corrupt PTE has been detected. Parameter 2 contains the address of
      the PTE. Parameters 3/4 contain the low/high parts of the PTE.
Arg2: ffffee01381e0b00
Arg3: 006f000000000000
Arg4: 0000000000000000
```

```
SYMBOL_NAME:  VSApiNt!VSSwapShortTable+136d

MODULE_NAME: VSApiNt

IMAGE_NAME:  VSApiNt.sys

STACK_COMMAND:  .thread ; .cxr ; kb

BUCKET_ID_FUNC_OFFSET:  136d

FAILURE_BUCKET_ID:  0x1a_41792_VSApiNt!VSSwapShortTable

OS_VERSION:  10.0.17134.1

BUILDLAB_STR:  rs4_release

OSPLATFORM_TYPE:  x64

OSNAME:  Windows 10

FAILURE_ID_HASH:  {6b73b256-ed5a-a5e1-ae4a-14c3f2eadd92}

Followup:     MachineOwner
---------
```

查看出错的线程的 callstack 信息，有 VSapiNt 和 TmXPFlt 参与。

```
5: kd> k
 # Child-SP          RetAddr           Call Site
00 fffff004`3af65ac8 fffff800`58c61150 nt!KeBugCheckEx
01 fffff004`3af65ad0 fffff800`58ad5789 nt!MiDeleteVa+0x189e00
02 fffff004`3af65be0 fffff800`58ad5b92 nt!MiWalkPageTablesRecursively+0x299
03 fffff004`3af65cc0 fffff800`58ad5b92 nt!MiWalkPageTablesRecursively+0x6a2
04 fffff004`3af65da0 fffff800`58ad5b92 nt!MiWalkPageTablesRecursively+0x6a2
05 fffff004`3af65e80 fffff800`58ad40a7 nt!MiWalkPageTablesRecursively+0x6a2
06 fffff004`3af65f60 fffff800`58acffc3 nt!MiWalkPageTables+0x1e7
07 fffff004`3af66050 fffff800`58f642c3 nt!MiDeleteVad+0x8d3
08 fffff004`3af66380 fffff800`58fd9110 nt!MiUnmapVad+0xa7
09 fffff004`3af663b0 fffff800`58fd8fbc nt!MiUnmapViewOfSection+0x120
0a fffff004`3af66490 fffff800`58fd8f10 nt!NtUnmapViewOfSectionEx+0x9c
0b fffff004`3af664e0 fffff800`58c3ff13 nt!NtUnmapViewOfSection+0xc
0c fffff004`3af66510 fffff800`58c31680 nt!KiSystemServiceCopyEnd+0x13
0d fffff004`3af666a8 fffff805`ea0783fd nt!KiServiceLinkage
0e fffff004`3af666b0 fffff805`ea0bb8e1 VSApiNt VSSwapShortTable+0x136d
0f fffff004`3af666e0 fffff805`ea0bf720 VSApiNt VSCloseFile+0x231
10 fffff004`3af667c0 fffff805`ea0aa13e VSApiNt TMCopySecurityDescriptor+0x670
11 fffff004`3af66840 fffff805`ea0aba1e VSApiNt VSIScanGetVirusInfoEx+0x6be
12 fffff004`3af668b0 fffff805`ea01e0d7 VSApiNt VSReadResource+0x48
13 fffff004`3af668f0 fffff805`e9ff4d4d VSApiNt VSScanResourceNTKD+0x13d57
14 fffff004`3af66920 fffff805`e9fee47b VSApiNt VSScanBP+0x597d
15 fffff004`3af66ef0 fffff805`ea01c2a4 VSApiNt VSRemoveWhiteChar+0x744b
16 fffff004`3af66fe0 fffff805`ea01ceaf VSApiNt VSScanResourceNTKD+0x11f2d
17 fffff004`3af67060 fffff805`ea01d67d VSApiNt VSScanResourceNTKD+0x12b2f
18 fffff004`3af670d0 fffff805`ea01e905 VSApiNt VSScanResourceNTKD+0x132fd
19 fffff004`3af67150 fffff805`e9fe7a21 VSApiNt VSScanResourceNTKD+0x14585
1a fffff004`3af671d0 fffff805`e9fe8e5f VSApiNt VSRemoveWhiteChar+0x9f1
1b fffff004`3af67330 fffff805`e9ef467d VSApiNt VSRemoveWhiteChar+0x1e28
1c fffff004`3af67650 fffff805`e9ef236a VSApiNt+0x467d
1d fffff004`3af676f0 fffff805`ea0add40 VSApiNt+0x236a
1e fffff004`3af677c0 fffff805`e6546cdc VSApiNt VSVirusScanFileW+0x190
1f fffff004`3af67850 fffff805`e6548711 TmXPFlt+0x26cdc
20 fffff004`3af67890 fffff805`e653015d TmXPFlt+0x28711
21 fffff004`3af678e0 fffff805`e6530c4d TmXPFlt+0x1015d
22 fffff004`3af67a20 fffff805`e65310b9 TmXPFlt+0x10c44
23 fffff004`3af67ae0 fffff800`58b77ae9 TmXPFlt+0x110b9
24 fffff004`3af67b10 fffff800`58c35b86 nt!PspSystemThreadStartup+0x47
25 fffff004`3af67b60 00000000`00000000 nt!KiStartSystemThread+0x16
```

查询 VSApiNt 模块情况，确认是属于亚信安全软件。

```
5: kd> lmvm VSApiNt
Browse full module list
start             end                 module name
fffff805`e9ef0000 fffff805`ea19d000   VSApiNt    (export symbols)       VSApiNt.sys
    Loaded symbol image file: VSApiNt.sys
    Image path: \??\C:\Program Files (x86)\Asiainfo Security\OfficeScan Client\VSApiNt.sys
    Image name: VSApiNt.sys
    Browse all global symbols  functions  data
    Timestamp:        Sun Sep 15 21:28:14 2019 (5D7E3C6E)
    CheckSum:         002B4254
    ImageSize:        002AD000
    Translations:     0000.04b0 0000.04e4 0409.04b0 0409.04e4
    Information from resource tables:
```

第二次 dump，BugCheck：0x139，并且提示应用程序 Ntrtscan.exe 异常（0xc0000409）

```
*******************************************************************************
*                                                                             *
*                        Bugcheck Analysis                                    *
*                                                                             *
*******************************************************************************

KERNEL_SECURITY_CHECK_FAILURE (139)
A kernel component has corrupted a critical data structure.  The corruption
could potentially allow a malicious user to gain control of this machine.
Arguments:
Arg1: 0000000000000003, A LIST_ENTRY has been corrupted (i.e. double remove).
Arg2: fffff58393626f80, Address of the trap frame for the exception that caused the bugcheck
Arg3: fffff58393626ed8, Address of the exception record for the exception that caused the bugcheck
Arg4: 0000000000000000, Reserved
```

```
TRAP_FRAME:  fffff58393626f80 -- (.trap 0xfffff58393626f80)
NOTE: The trap frame does not contain all registers.
Some register values may be zeroed or incorrect.
rax=ffff800490534a20 rbx=0000000000000000 rcx=0000000000000003
rdx=0000000000000000 rsi=0000000000000000 rdi=0000000000000000
rip=fffff801cc98ce55 rsp=fffff58393627110 rbp=fffff58393627199
 r8=0000000000000000  r9=0000000000000001 r10=0000000000000001
r11=0000000000000002 r12=0000000000000000 r13=0000000000000000
r14=0000000000000000 r15=0000000000000000
iopl=0         nv up ei ng nz na po cy
nt!ExAllocatePoolWithTag+0x1a45:
fffff801`cc98ce55 cd29            int     29h
Resetting default scope

EXCEPTION_RECORD:  fffff58393626ed8 -- (.exr 0xfffff58393626ed8)
ExceptionAddress: fffff801cc98ce55 (nt!ExAllocatePoolWithTag+0x0000000000001a45)
   ExceptionCode: c0000409 (Security check failure or stack buffer overrun)
  ExceptionFlags: 00000001
NumberParameters: 1
   Parameter[0]: 0000000000000003
Subcode: 0x3 FAST_FAIL_CORRUPT_LIST_ENTRY

BLACKBOXPNP: 1 (!blackboxpnp)


PROCESS_NAME:  Ntrtscan.exe

ERROR_CODE: (NTSTATUS) 0xc0000409 - <Unable to get error code text>

EXCEPTION_CODE_STR:  c0000409

EXCEPTION_PARAMETER1:  0000000000000003

DEVICE_OBJECT: ffffffff8000a2fc

EXCEPTION_STR:  0xc0000409
```

查看当前报错的线程情况，它属于 Ntrtscan.exe 进程

```
7: kd> !thread
THREAD ffff9e00839e8700  Cid 1154.38e8  Teb: 00000000002a6000 Win32Thread: 0000000000000000 RUNNING on processor 7
IRP List:
    ffff9e009eb65010: (0006,0508) Flags: 00060800  Mdl: 00000000
    ffff9e009e180010: (0006,0508) Flags: 00000884  Mdl: 00000000
    ffff9e00816c8010: (0006,0118) Flags: 00060000  Mdl: 00000000
Not impersonating
DeviceMap                 ffff80047a618a40
Owning Process            ffff9e0083c8f580       Image:         Ntrtscan.exe
Attached Process          N/A            Image:         N/A
Wait Start TickCount      10779509       Ticks: 0
Context Switch Count      639553         IdealProcessor: 7
UserTime                  00:00:23.625
KernelTime                00:11:47.062
Win32 Start Address ntrtscan (0x00007ff731363930)
Stack Init fffff58393627fd0 Current fffff5839326e0a0
Base fffff58393628000 Limit fffff58393621000 Call 0000000000000000
Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
```

查看当前出错线程的 callstack，与第一个 dump 一样有 VSapiNt 和 TmXPFlt 参与。

```
26 fffff583`9326dc60 fffff801`ccb7dbe3 nt!IofCallDriver+0x59
27 fffff583`9326dca0 fffff801`ccb6a2ab nt!IopParseDevice+0x773
28 fffff583`9326de70 fffff801`ccb7bd1f nt!ObpLookupObjectName+0x73b
29 fffff583`9326e050 fffff801`ccbe1805 nt!ObOpenObjectByNameEx+0x1df
2a fffff583`9326e190 fffff801`ccbe13f9 nt!IopCreateFile+0x3f5
2b fffff583`9326e230 fffff801`cc83df13 nt!NtCreateFile+0x79
2c fffff583`9326e2c0 fffff801`cc82f680 nt!KiSystemServiceCopyEnd+0x13
2d fffff583`9326e4c8 fffff804`63749020 nt!KiServiceLinkage
2e fffff583`9326e4d0 fffff804`637493d5 VSApiNt+0x189020
2f fffff583`9326e560 fffff804`6378d5c6 VSApiNt+0x1893d5
30 fffff583`9326e600 fffff804`6377c682 VSApiNt+0x1cd5c6
31 fffff583`9326e730 fffff804`6377d466 VSApiNt+0x1bc682
32 fffff583`9326e7b0 fffff804`636f02f5 VSApiNt+0x1bd466
33 fffff583`9326e7f0 fffff804`636f0bc6 VSApiNt+0x1302f5
34 fffff583`9326e830 fffff804`636c305a VSApiNt+0x130bc6
35 fffff583`9326e8c0 fffff804`636ecff5 VSApiNt+0x10305a
36 fffff583`9326ee90 fffff804`636ed464 VSApiNt+0x12cff5
37 fffff583`9326ef00 fffff804`636ed61c VSApiNt+0x12d464
38 fffff583`9326ef80 fffff804`636ee905 VSApiNt+0x12d61c
39 fffff583`9326f000 fffff804`636e0581 VSApiNt+0x12e905
3a fffff583`9326f080 fffff804`635c48e8 VSApiNt+0x120581
3b fffff583`9326f2b0 fffff804`635c236a VSApiNt+0x48e8
3c fffff583`9326f350 fffff804`6377dd40 VSApiNt+0x236a
3d fffff583`9326f420 fffff804`63956cdc VSApiNt+0x1bdd40
3e fffff583`9326f4b0 fffff804`63958711 TmXPFlt+0x26cdc
3f fffff583`9326f4f0 fffff804`6395988c TmXPFlt+0x28711
40 fffff583`9326f540 fffff804`6394f658 TmXPFlt+0x2988c
41 fffff583`9326f5f0 fffff804`63955c80 TmXPFlt+0x1f658
42 fffff583`9326f640 fffff804`6393501d TmXPFlt+0x25c80
43 fffff583`9326f6a0 fffff801`cc6dcdb9 TmXPFlt+0x501d
44 fffff583`9326f700 fffff801`ccb651ab nt!IofCallDriver+0x59
45 fffff583`9326f740 fffff801`ccb710ef nt!IopSynchronousServiceTail+0x1ab
46 fffff583`9326f7f0 fffff801`ccb71896 nt!IopXxxControlFile+0x66f
47 fffff583`9326f920 fffff801`cc83df13 nt!NtDeviceIoControlFile+0x56
48 fffff583`9326f990 00007ff9`31b8a074 nt!KiSystemServiceCopyEnd+0x13
49 00000000`7828ae38 00007ff9`2ed3776a ntdll!NtDeviceIoControlFile+0x14
4a 00000000`7828ae40 00007ff9`31803d30 KERNELBASE!DeviceIoControl+0x1da
4b 00000000`7828aeb0 00007ff7`3152ab2c KERNEL32!DeviceIoControlImplementation+0x80
4c 00000000`7828af00 00000000`00000048 ntrtscan!GetAppPath+0x70b8c
4d 00000000`7828af08 00000000`a028448b 0x48
4e 00000000`7828af10 00000000`00000000 0xa028448b
```

Ntrtscan.exe 属于亚信安全软件。

```
7: kd> lmvm ntrtscan
Browse full module list
start             end                 module name
00007ff7`31140000 00007ff7`3188d000   ntrtscan   (export symbols)       ntrtscan.exe
    Loaded symbol image file: ntrtscan.exe
    Image path: C:\Program Files (x86)\Asiainfo Security\OfficeScan Client\ntrtscan.exe
    Image name: ntrtscan.exe
    Browse all global symbols  functions  data
    Timestamp:        Tue Jun  5 12:39:08 2018 (5B1613EC)
    CheckSum:         0072A31B
    ImageSize:        0074D000
    File version:     13.0.0.1733
    Product version:  13.0.0.1733
    File flags:       0 (Mask 3F)
    File OS:          40004 NT Win32
    File type:        1.0 App
    File date:        00000000.00000000
    Translations:     0409.04b0
    Information from resource tables:
        CompanyName:      trend_company_name
        ProductName:      trend_product_name
        ProductVersion:   13.0
        FileVersion:      13.0.0.1733
        PrivateBuild:     trend_private_build
        SpecialBuild:     trend_special_build
        FileDescription:  Asiainfo Security Common Client Real-time Scan Service (64-bit)
        LegalCopyright:   Copyright (C) 1998-2007
        LegalTrademarks:  trend_legal_trademarks
```

两个 dump 虽然 BugCheck 代码不一样，但是从出错的线程的 callstack 信息查看，是由亚信安全软件引起的蓝屏。

查找相关信息，确认 Officescan 与趋势有关，因为亚信收购了趋势中国的全部业务，并推出了亚信安全。

在趋势官网查找到一篇文档说明了 Officescan 在某些情况下有可能出现蓝屏情况。

https://success.trendmicro.com/solution/1119990-blue-screen-of-death-bsod-occurred-on-windows-10-april-2018-update

请您按照此文档中的解决方案测试是否能缓解问题。

2. Select endpoints with the Windows 10 April 2018 Update, apply the following exclusions via **Settings** > **Behavior Monitoring Settings** > **Exceptions** > **Add to Approved List**.
   Add the following processes:
   - C:\Program Files\WindowsApps\Microsoft.Messaging_*\SkypeHost.exe
   - C:\Windows\SystemApps*\SearchUI.exe
   - C:\Windows\ImmersiveControlPanel\SystemSettings.exe
   - C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_*\HxTsr.exe
   - C:\Windows\SystemApps\Microsoft.LockApp_*\LockApp.exe
   - C:\Windows\SystemApps\Microsoft.MicrosoftEdge_*\MicrosoftEdge.exe
3. Save and exit.

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 CMIT

发件人: Wei Liang
发送时间: 2021 年 9 月 6 日 14:54
收 件 人 : ' 吴 毓 杰 ' <win10sup@sdc.icbc.com.cn>; 'hongbo@icbc.com.cn' <hongbo@icbc.com.cn>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: [案例号: CAS-04716-C3F2K9] % |P3|ICBC|总行 win10 神州网信政府版电脑蓝屏 % 初次响应 CMIT:0001032

洪先生 您好:

我已经收到您发送的新的 dump 日志，正在对此日志进行分析，有任何进展会及时和您联系。

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: 2021 年 9 月 1 日 18:04
收 件 人 : 吴 毓 杰 <win10sup@sdc.icbc.com.cn>; 'hongbo@icbc.com.cn' <hongbo@icbc.com.cn>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: [案例号: CAS-04716-C3F2K9] % |P3|ICBC|总行 win10 神州网信政府版电脑蓝屏 % 初次响应 CMIT:0001032

洪先生 您好:

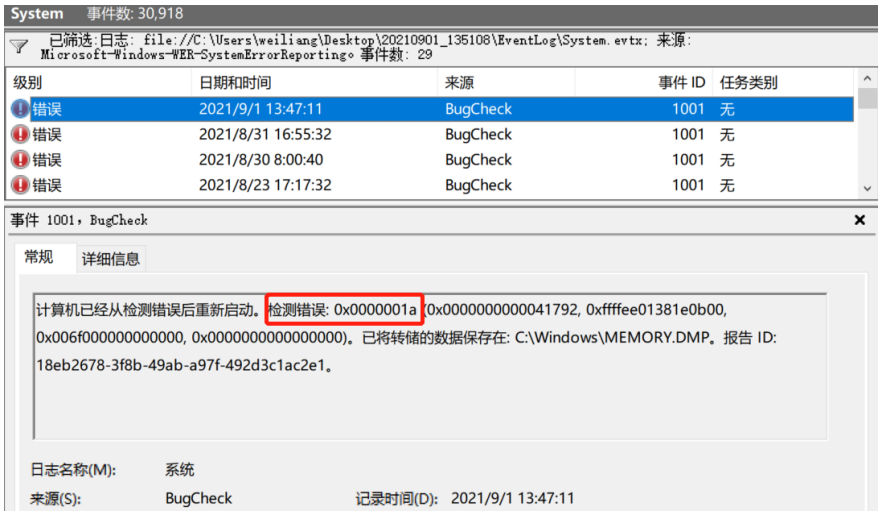
根据刚才的电话沟通，我谨在此阐述我们双方针对这个问题所涉及范围界定:

问题定义:
总行 Windows 10 神州网信政府版 V0-H 不定时出现蓝屏。

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。

查看您上传的系统日志，可以发现不定时出现蓝屏报错，且有不同的 BugCheck 报错代码。



基于您上传的 dump 日志分析，查看出现蓝屏时的 call_stack 信息，显示与 VSApiNt.sys 有关。

```
SYMBOL_NAME:  VSApiNt!VSSwapShortTable+136d

MODULE_NAME: VSApiNt

IMAGE_NAME:  VSApiNt.sys

STACK_COMMAND:  .thread ; .cxr ; kb

BUCKET_ID_FUNC_OFFSET:  136d

FAILURE_BUCKET_ID:  0x1a_41792_VSApiNt!VSSwapShortTable

OS_VERSION:  10.0.17134.1

BUILDLAB_STR:  rs4_release

OSPLATFORM_TYPE:  x64

OSNAME:  Windows 10

FAILURE_ID_HASH:  {6b73b256-ed5a-a5e1-ae4a-14c3f2eadd92}
```

查看 VSApiNt.sys 模块情况，确认是亚信安全软件的一个组件。

```
5: kd> lmvm VSApiNt
Browse full module list
start             end                 module name
fffff805`e9ef0000 fffff805`ea19d000   VSApiNt    (export symbols)       VSApiNt.sys
    Loaded symbol image file: VSApiNt.sys
    Image path: \??\C:\Program Files (x86)\Asiainfo Security\OfficeScan Client\VSApiNt.sys
    Image name: VSApiNt.sys
    Browse all global symbols  functions  data
    Timestamp:        Sun Sep 15 21:28:14 2019 (5D7E3C6E)
    CheckSum:         002B4254
    ImageSize:        002AD000
    Translations:     0000.04b0 0000.04e4 0409.04b0 0409.04e4
    Information from resource tables:
```

为方便进一步分析此问题，如果条件允许的话，请卸载相关的安控杀毒软件，即 Asiainfo Security，供排错分析。

如果无法做这些操作测试，请您多次收集新的蓝屏 dump 日志，进行分析对比确认。

新的 dump 日志，请 @吴毓杰 帮忙上传到 sftp 服务器。

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 CMIT

发件人: Wei Liang <weiliang@cmgos.com>
发送时间: 2021 年 9 月 1 日 15:23
收件人: 吴毓杰 <win10sup@sdc.icbc.com.cn>
抄送: Wei Liang <weiliang@cmgos.com>
主题: [案例号：CAS-04716-C3F2K9] % |P3|ICBC|总行 win10 神州网信政府版电脑蓝屏 % 初次响应 CMIT:0001032

吴毓杰 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-04716-C3F2K9 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
