高先生 您好：

感谢您的电话接听。
经过您的确认，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：

V0-H 版系统离线安装 KB4535680 补丁失败，需提供具体安装方法。

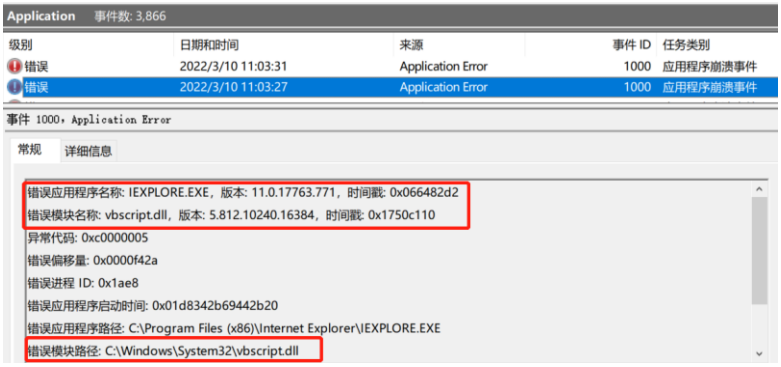
问题总结：

用户测试确认是 360 安全卫士导致使用网银 U 盾时 IE 异常退出，可以关闭案例。

问题分析过程：

1、先查看系统应用日志和系统日志，确认问题基本情况。

这个案例显示了应用异常退出的 eventid 1000 的事件日志，可以看到导致异常的模块是 vbscript.dll。



2、vbscript.dll 是系统提供的组件，此时需要进一步排查，使用 procdump 工具抓取应用异常退出时刻的 dump，尝试抓取导致应用异常退出的具体模块。

将 procdump.exe 复制到 C:\dumps 目录，以**管理员权限**打开 cmd 命令行，定位到 C:\dumps，运行以下命令配置 procdump 自动生成转储文件。

```
cd c:\dumps
procdump.exe -ma -i
```

3、当抓取了应用异常退出时的 dmp 文件，可以使用 windbg 工具分析对应的 dmp 文件。（windbg 工具基本使用可以查找相应的资料学习）

```
0:009> !lt
# DbgID ThdID Wait Function                                User Kernel Info     TEB      Create
Time
== ===== ===== ============================================ ===== ====== ======== ========
==========================
```

```
       0  230c win32u!NtUserMsgWaitForMultipleObjectsEx+0xc
250ms   31ms          007d8000 03/11/2022 02:36:13.016 上午
       1  2a00 ntdll!NtWaitForWorkViaWorkerFactory+0xc          0      0          007db000 03/11/2
022 02:36:13.032 上午
       2   794 ntdll!NtWaitForWorkViaWorkerFactory+0xc          0   15ms          007de000 03/11/2
022 02:36:13.032 上午
       3  2d6c ntdll!NtWaitForWorkViaWorkerFactory+0xc          0      0          007e1000 03/11/2
022 02:36:13.032 上午
       4  22e4 win32u!NtUserMsgWaitForMultipleObjectsEx+0xc     0      0          007e4000 03/11/2
022 02:36:13.282 上午
       5  2ce4 ntdll!NtWaitForWorkViaWorkerFactory+0xc          0   46ms          007e7000 03/11/2
022 02:36:13.376 上午
       6   bb8 ntdll!NtWaitForWorkViaWorkerFactory+0xc       31ms      0          007ea000 03/11/2
022 02:36:13.379 上午
       7  2e48 ntdll!NtWaitForWorkViaWorkerFactory+0xc          0      0          007ed000 03/11/2
022 02:36:13.379 上午
       8  2f68 combase!WaitCoalesced+0xb5                       0      0          007f0000 03/11/2
022 02:36:13.380 上午
->     9  3074 kernel32!WerpReportFaultInternal+0x3b7       281ms  328ms Event... 007f3000 03/11/2
022 02:36:13.382 上午
      10  1df8 ntdll!NtWaitForWorkViaWorkerFactory+0xc          0      0          007f6000 03/11/2
022 02:36:13.552 上午
      11  33b0 crypt32!ILS_WaitForThreadProc+0x26               0      0          007f9000 03/11/2
022 02:36:13.564 上午
      12    e8 ntdll!NtWaitForWorkViaWorkerFactory+0xc          0      0          007fc000 03/11/2
022 02:36:13.565 上午
```

列出所有的线程，显示了有一个线程出现 Fault 的信息

```
0:009> .lastevent
Last event: 1f1c.3074: Access violation - code c0000005 (first/second chance not available)
  debugger time: Fri Mar 11 14:21:12.527 2022 (UTC + 8:00)
```

查看其 event 信息，显示 Access violation 内存访问冲突，是这个错误导致了应用异常退出。

```
0:009> !mex.t -t 0x3074
DbgID ThreadID        User Kernel Create Time (UTC)
9     3074 (0n12404) 281ms  328ms 03/11/2022 02:36:13.382 上午

# Child-SP Return   Call Site
0 05895758 75e3abc3 ntdll!NtWaitForMultipleObjects+0xc
1 0589575c 75e3aa78 KERNELBASE!WaitForMultipleObjectsEx+0x133
2 058958f0 75645982 KERNELBASE!WaitForMultipleObjects+0x18
3 0589590c 756455b1 kernel32!WerpReportFaultInternal+0x3b7
4 058959b8 7561be39 kernel32!WerpReportFault+0x9d
5 058959d4 75ecb2df kernel32!BasepReportFault+0x19
6 058959dc 72074b4c KERNELBASE!UnhandledExceptionFilter+0x2df
7 05895a7c 77942fc7 safemon!DllUnregisterServer+0x2eb2c
8 05895aa4 779066ad ntdll!__RtlUserThreadStart+0x3c919
9 0589f8a4 00000000 ntdll!_RtlUserThreadStart+0x1b
```

查看这个线程的 call Stack 具体信息，CallStack 信息从下往上查看，显示了 safemon 模块 DllUnregisterServer 导致了 UnhandledExceptionFilter，最终 WerpReportFaultInternal。

这里考虑是 safemon 模块导致了应用异常退出，进一步测试先删除此模块验证应用运行情况。

```
0:009> lmvm safemon
Browse full module list
start    end        module name
72040000 7227d000   safemon    (export symbols)       safemon.dll
    Loaded symbol image file: safemon.dll
```

```
Image path: C:\Program Files (x86)\360\360Safe\safemon\safemon.dll
Image name: safemon.dll
Browse all global symbols  functions  data
Timestamp:        Tue Dec 28 15:39:35 2021 (61CABF37)
CheckSum:         002280E1
ImageSize:        0023D000
File version:     8.6.0.3660
Product version:  8.6.0.3660
File flags:       0 (Mask 17)
File OS:          4 Unknown Win32
File type:        2.0 Dll
File date:        00000000.00000000
Translations:     0804.04b0
Information from resource tables:
    CompanyName:      360.cn
    ProductName:      360 安全卫士
    InternalName:     safemon.dll
    OriginalFilename: safemon.dll
    ProductVersion:   8.6.0.3660
    FileVersion:      8.6.0.3660
    FileDescription:  360 安全卫士 网盾防护模块
    LegalCopyright:
```

查看 safemon 模块是 360 安全卫士的组件，先卸载 360 安全卫士，再测试在 IE 中使用网银 U 盾情况。

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.
服务电话： 4008180055
电子邮箱： weiliang@cmgos.com
官方网站： www.cmgos.com

发件人: Wei Liang
发送时间: 2022 年 3 月 14 日 10:44
收件人: 高先生
抄送: Case_Notification
主题: 答复: [案例号: CAS-05833-J0B0R6] % VDI 用户-北京牡丹电子集团有限责任公司用户反馈使用网银 U 盾调用 IE 时导致 IE 崩溃问题 % 初次响应 CMIT:0001754

高先生 您好：

刚刚给您的电话没有接通。
来信是想咨询当前案例进展状况。测试卸载 360 安全软件后，使用网银 U 盾时 IE 是否会异常退出？
如果针对当前案件还有需要我们帮助的地方, 欢迎随时通过邮件或热线电话联系我们。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务电话： 4008180055
电子邮箱： weiliang@cmgos.com
官方网站： www.cmgos.com

发件人: Wei Liang
发送时间: 2022 年 3 月 11 日 14:27
收件人: 高先生
抄送: Case_Notification
主题: 回复: [案例号: CAS-05833-J0B0R6] % VDI 用户-北京牡丹电子集团有限责任公司用户反馈使用网银 U 盾调用 IE 时导致 IE 崩溃问题 % 初次响应 CMIT:0001754

高先生 您好:

感谢您的电话接听。
当前生成的 dmp 文件显示出现 IE 异常退出是 safemon.dll 导致的，safemon.dll 是 360 安全卫士的组件（C:\Program Files (x86)\360\360Safe\safemon\safemon.dll）。
请您测试**卸载 360 安全卫士**，确认计算机上**没有 360 安全卫士残留**后，再次测试在 IE 中使用网银 U 盾是否有 IE 异常退出问题。
（测试时按照上一封邮件提前配置 procdump 工具，确保出现问题时可以及时生成 dmp 文件。）

dmp 文件详细分析：

```
0:009> !lt
# DbgID ThdID Wait Function                                  User Kernel Info     TEB      Create Time
== ===== ===== ============================================ ===== ====== ======== ======== ========================
       0  230c win32u!NtUserMsgWaitForMultipleObjectsEx+0xc 250ms   31ms          007d8000 03/11/2022
02:36:13.016 上午
       1  2a00 ntdll!NtWaitForWorkViaWorkerFactory+0xc          0      0          007db000 03/11/2022
02:36:13.032 上午
       2   794 ntdll!NtWaitForWorkViaWorkerFactory+0xc          0   15ms          007de000 03/11/2022
02:36:13.032 上午
       3  2d6c ntdll!NtWaitForWorkViaWorkerFactory+0xc          0      0          007e1000 03/11/2022
02:36:13.032 上午
       4  22e4 win32u!NtUserMsgWaitForMultipleObjectsEx+0xc     0      0          007e4000 03/11/2022
02:36:13.282 上午
       5  2ce4 ntdll!NtWaitForWorkViaWorkerFactory+0xc          0   46ms          007e7000 03/11/2022
02:36:13.376 上午
       6   bb8 ntdll!NtWaitForWorkViaWorkerFactory+0xc       31ms      0          007ea000 03/11/2022
02:36:13.379 上午
       7  2e48 ntdll!NtWaitForWorkViaWorkerFactory+0xc          0      0          007ed000 03/11/2022
02:36:13.379 上午
       8  2f68 combase!WaitCoalesced+0xb5                       0      0          007f0000 03/11/2022
02:36:13.380 上午
->     9  3074 kernel32!WerpReportFaultInternal+0x3b7       281ms  328ms Event... 007f3000 03/11/2022
02:36:13.382 上午
      10  1df8 ntdll!NtWaitForWorkViaWorkerFactory+0xc          0      0          007f6000 03/11/2022
02:36:13.552 上午
```

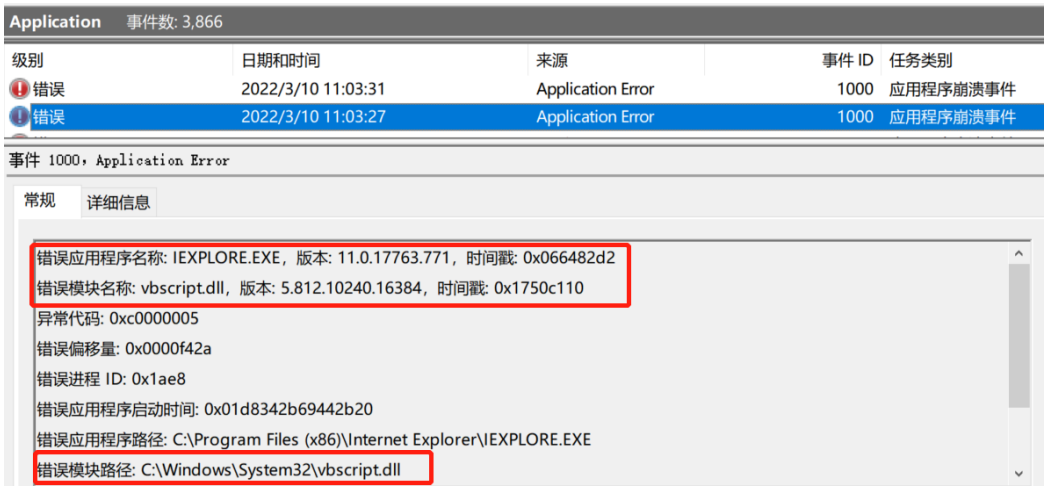
```
      11  33b0 crypt32!ILS_WaitForThreadProc+0x26              0      0          007f9000 03/11/2022
02:36:13.564 上午
      12    e8 ntdll!NtWaitForWorkViaWorkerFactory+0xc         0      0          007fc000 03/11/2022
02:36:13.565 上午

0:009> .lastevent
Last event: 1f1c.3074: Access violation - code c0000005 (first/second chance not available)
  debugger time: Fri Mar 11 14:21:12.527 2022 (UTC + 8:00)
0:009> !mex.t -t 0x3074
DbgID ThreadID        User Kernel Create Time (UTC)
9     3074 (0n12404) 281ms  328ms 03/11/2022 02:36:13.382 上午

# Child-SP Return   Call Site
0 05895758 75e3abc3 ntdll!NtWaitForMultipleObjects+0xc
1 0589575c 75e3aa78 KERNELBASE!WaitForMultipleObjectsEx+0x133
2 058958f0 75645982 KERNELBASE!WaitForMultipleObjects+0x18
3 0589590c 756455b1 kernel32!WerpReportFaultInternal+0x3b7
4 058959b8 7561be39 kernel32!WerpReportFault+0x9d
5 058959d4 75ecb2df kernel32!BasepReportFault+0x19
6 058959dc 72074b4c KERNELBASE!UnhandledExceptionFilter+0x2df
7 05895a7c 77942fc7 safemon!DllUnregisterServer+0x2eb2c
8 05895aa4 779066ad ntdll!__RtlUserThreadStart+0x3c919
9 0589f8a4 00000000 ntdll!_RtlUserThreadStart+0x1b

0:009> lmvm safemon
Browse full module list
start    end        module name
72040000 7227d000   safemon    (export symbols)       safemon.dll
    Loaded symbol image file: safemon.dll
    Image path: C:\Program Files (x86)\360\360Safe\safemon\safemon.dll
    Image name: safemon.dll
    Browse all global symbols  functions  data
    Timestamp:        Tue Dec 28 15:39:35 2021 (61CABF37)
    CheckSum:         002280E1
    ImageSize:        0023D000
    File version:     8.6.0.3660
    Product version:  8.6.0.3660
    File flags:       0 (Mask 17)
    File OS:          4 Unknown Win32
    File type:        2.0 Dll
    File date:        00000000.00000000
    Translations:     0804.04b0
    Information from resource tables:
        CompanyName:      360.cn
        ProductName:      360 安全卫士
        InternalName:     safemon.dll
        OriginalFilename: safemon.dll
        ProductVersion:   8.6.0.3660
        FileVersion:      8.6.0.3660
        FileDescription:  360 安全卫士 网盾防护模块
        LegalCopyright:
```

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: 2022 年 3 月 10 日 16:57
收件人: '高先生' <gaos@peony.cn>
抄送: Case_Notification <Case_Notification@cmgos.com>
主题: 回复: [案例号: CAS-05833-J0B0R6] % VDI 用户-北京牡丹电子集团有限责任公司用户反馈使用网银 U 盾调用 IE 时导致 IE 崩溃问题 % 初次响应 CMIT:0001754

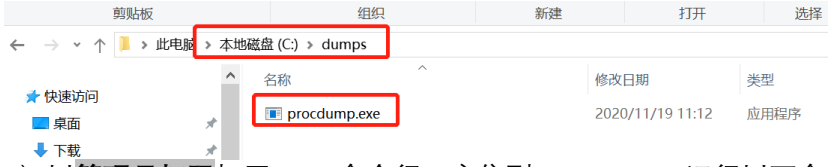
高先生 您好:

感谢您的电话接听。
从您提供的应用事件日志中显示 IE 异常退出是由 vbscript.dll 模块引起的，它是操作系统的应用扩展模块。

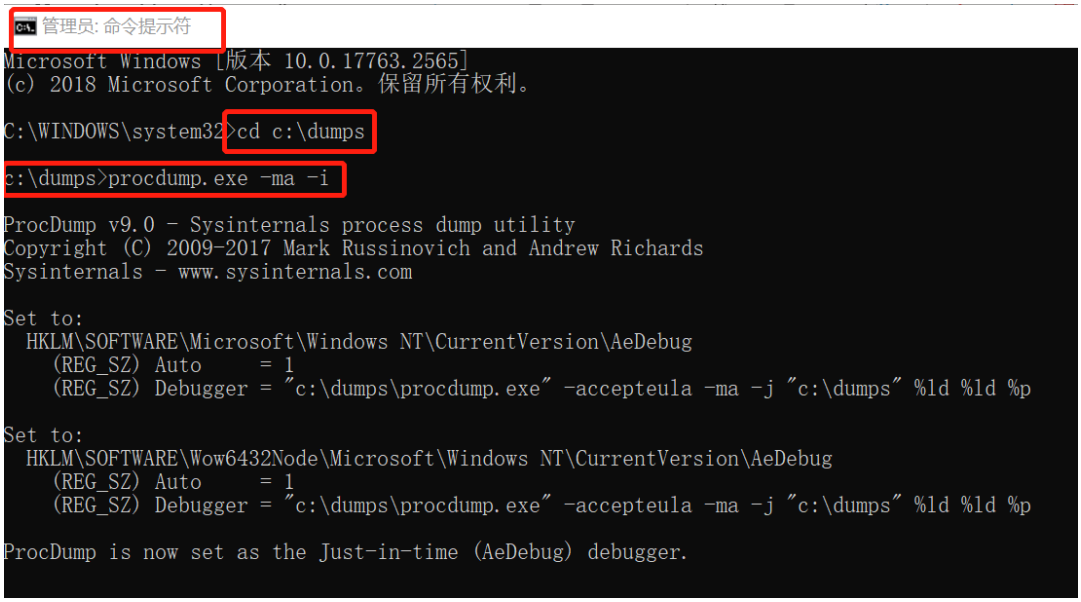


要进一步分析这个问题，需要抓取 IE 异常退出时的转储文件。

请您按照以下方式配置，**并复现 IE 异常退出问题**。
1）下载附件中的 procdump 工具并解压。
2）在故障机创建文件目录 C:\dumps，将 procdump.exe 复制到 C:\dumps 目录。



3）以**管理员权限**打开 cmd 命令行，定位到 C:\dumps，运行以下命令配置 procdump 自动生成转储文件。
cd c:\dumps
procdump.exe -ma -i

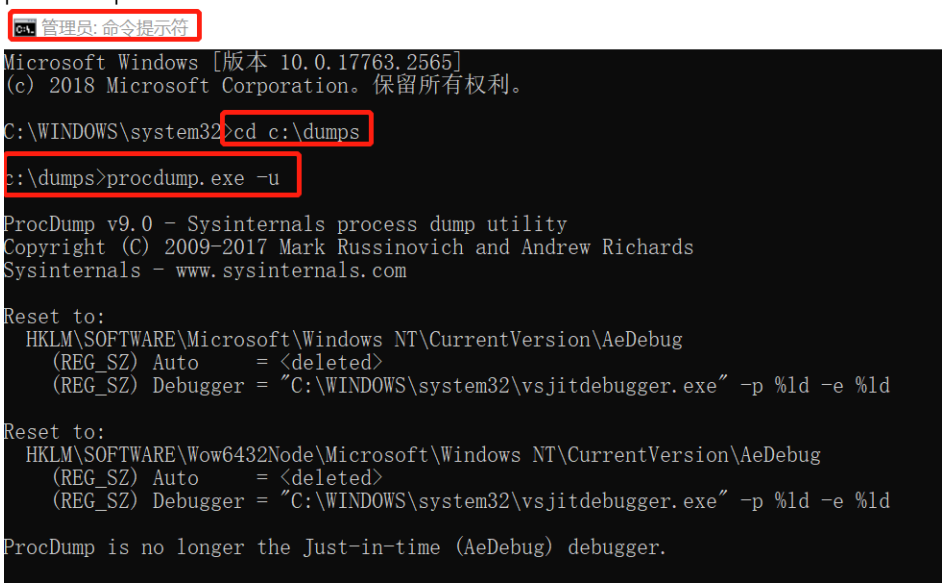


4）连接 U 盾操作，复现 IE 异常退出的问题。

5）以管理员权限打开 cmd 命令行，定位到 C:\dumps，运行以下命令取消 procdump 配置。

cd c:\dumps

procdump.exe -u



6）将 C:\dumps 目录下生成的 dmp 文件压缩，并通过 CDUC 上传。

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: 2022 年 3 月 9 日 17:06
收件人: 高先生 <gaos@peony.cn>
抄送: Case_Notification <Case_Notification@cmgos.com>
主题: 回复: [案例号: CAS-05833-J0B0R6] % VDI 用户-北京牡丹电子集团有限责任公司用户反馈使用网银 U 盾调用 IE 时导致 IE 崩溃问题 % 初次响应 CMIT:0001754

高先生 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:
财务电脑使用网银 U 盾调用 IE 时，导致 IE 崩溃报错，这个问题不规律发生。

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。

针对您这个问题，请您按照以下方法帮忙收集相关系统日志进行分析。
1）下载附件中的 CMGELogCollector.zip，解压后运行 CMGELogCollector.exe，勾选全部选项，点击“收集”，运行几分钟后会在桌面**生成日志压缩包**。

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。如果出现类似错误提示，点击后退即可。

用户名：BJMDDZJT

密码：BJMDDZJT

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。

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: 2022 年 3 月 9 日 16:52
收件人: 高先生 <gaos@peony.cn>
抄送: Wei Liang <weiliang@cmgos.com>
主题: [案例号：CAS-05833-J0B0R6] % VDI 用户-北京牡丹电子集团有限责任公司用户反馈使用网银 U 盾调用 IE 时导致 IE 崩溃问题 % 初次响应 CMIT:0001754

高先生 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-05833-J0B0R6 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

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”。