已了解，多谢李工，我们会联系 TMS 厂商进行确认，感谢支持。

李粤
工行软件开发中心
TEL：0756-3395361(长响转手机)

发件人: Li Qi <liqi@cmgos.com>
收件人: 吴毓杰 <win10sup@sdc.icbc.com.cn>, "liyue@sdc.icbc.com.cn" <liyue@sdc.icbc.com.cn>
抄送: CRM Case Email <casemail@cmgos.com>, Liu Wei <liuwei@cmgos.com>, Li Xin <lixin@cmgos.com>, Qi Feng <qifeng@cmgos.com>, Wang Dan <wangdan@cmgos.com>, Wang Wenlei <wangwl@cmgos.com>
日期: 2020/08/19 14:39
主题: 回复: [案例号: CAS-02811-T4V2H7] % |P3|ICBC|插拔 U 盘设备时电脑蓝屏 % 初次响应 CMIT:0001729

Hi，粤总:

请帮忙毓杰邮件确认该问题的分析结果，谢谢

李琦 Li Qi
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 Email: liqi@cmgos.com

发件人: Li Qi
发送时间: 2020 年 8 月 19 日 9:23
收件人: 吴毓杰 <win10sup@sdc.icbc.com.cn>
抄送: CRM Case Email <casemail@cmgos.com>; Liu Wei <liuwei@cmgos.com>; Li Xin <lixin@cmgos.com>; Qi Feng <qifeng@cmgos.com>; Wang Dan <wangdan@cmgos.com>; Wang Wenlei <wangwl@cmgos.com>
主题: 回复: [案例号: CAS-02811-T4V2H7] % |P3|ICBC|插拔 U 盘设备时电脑蓝屏 % 初次响应 CMIT:0001729

吴先生，您好:

如之前沟通，根据已收集的 dump，针对此问题，目前已分析完毕。请您邮件确认此问题分析结果:

Case No：CAS-02811-T4V2H7

问题描述：
=====================
用户反馈，插拔 U 盘设备时电脑蓝屏

问题分析：
======================
造成此问题是由于开启 special pool 之后，detect 到有驱动组件在进行违规操作导致，bugcheck detail 如下：

```
Bugcheck details
=============================================
DRIVER_VERIFIER_DETECTED_VIOLATION (c4)
A device driver attempting to corrupt the system has been caught.  This is
because the driver was specified in the registry as being suspect (by the
administrator) and the kernel has enabled substantial checking of this driver.
If the driver attempts to corrupt the system, bugchecks 0xC4, 0xC1 and 0xA will
be among the most commonly seen crashes.
Arguments:
Arg1: 00000000000000f6, Referencing user handle as KernelMode.
Arg2: 00000000000024b0, Handle value being referenced.
Arg3: ffffe6841fa57580, Address of the current process.
Arg4: fffff8089d90aa39, Address inside the driver that is performing the incorrect reference.
```

```
Crashing Stack
=============================================
Process                    Thread         CID      UserTime KernelTime ContextSwitches Wait Reason
Time State           COM-Initialized
explorer.exe (ffffe6841fa57580) ffffe6841cf4f080 1944.c04       0s      31ms             5
WrPageIn      0s Running on CPU 1 APTKIND_APARTMENTTHREADED (STA)
```

具体的 call stack 信息如下：

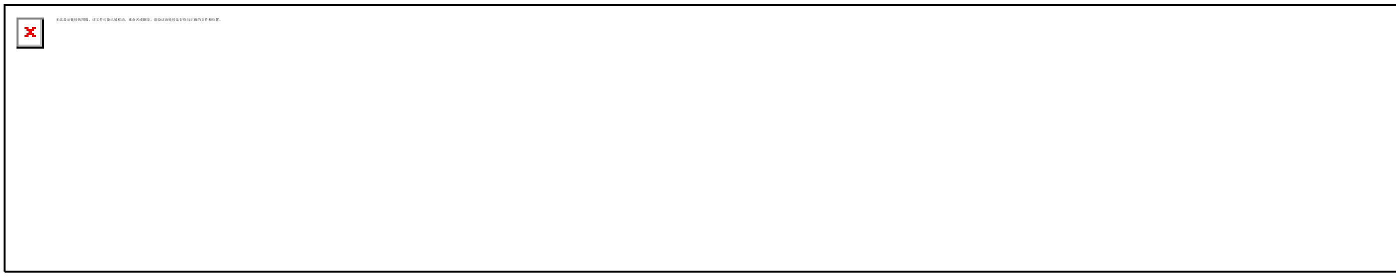
```
0 ffff9903d62c66f8 fffff80162c3e483 nt!KeBugCheckEx+0x0
 1 ffff9903d62c6700 fffff80162c469d4 nt!VerifierBugCheckIfAppropriate+0xdf
 2 ffff9903d62c6740 fffff80162ad2f5d nt!VfCheckUserHandle+0x1d4
 3 ffff9903d62c6830 fffff80162930b9e
nt!ObpReferenceObjectByHandleWithTag+0x1a23ad
 4 (Inline)        ---------------- nt!ObReferenceObjectByHandleWithTag+0x2a
 5 ffff9903d62c68c0 fffff801628dff93 nt!ObReferenceObjectByHandle+0x2e
 6 (Inline)        ---------------- nt!_ObReferenceObjectByHandle+0x24
 7 ffff9903d62c6910 fffff801625da143 nt!NtQuerySymbolicLinkObject+0xf3
 8 ffff9903d62c6990 fffff801625cd4c0 nt!KiSystemServiceCopyEnd+0x13
 9 ffff9903d62c6b28 fffff80162c575d6 nt!KiServiceLinkage+0x0
 a ffff9903d62c6b30 fffff8089d90aa39 nt!VfZwQuerySymbolicLinkObject+0x56
 b ffff9903d62c6b60 fffff8089d90ab92 gscfmgr+0xaa39
 c ffff9903d62c6ec0 fffff8089d905c0d gscfmgr+0xab92
 d ffff9903d62c6ef0 fffff8089c3dae29 gscfmgr+0x5c0d
```

向上追溯 gscfmgr 的行为，可以看到调用 ObpReferenceObjectByHandleWithTag

```
1: kd> .frame /r 0x3; !mex.x
03 ffff9903`d62c6830 fffff801`62930b9e nt!ObpReferenceObjectByHandleWithTag+0x1a23ad
[minkernel\ntos\ob\obref.c @ 1918]
rax=fffff8089d90aa39 rbx=ffffe6840f8b09e0 rcx=00000000000000c4
rdx=00000000000000f6 rsi=0000000000000000 rdi=ffffe6841fa57580
rip=fffff80162ad2f5d rsp=ffff9903d62c6830 rbp=ffff9903d62c6a10
r8=00000000000024b0  r9=ffffe6841fa57580 r10=0000000000000004
r11=ffff9903d62c67d0 r12=ffff9903d62c6940 r13=0000000000000000
r14=ffffe6841cf4f080 r15=00000000000024b0
iopl=0         nv up ei pl zr na po nc
cs=0010  ss=0018  ds=002b  es=002b  fs=0053  gs=002b             efl=00000246
nt!ObpReferenceObjectByHandleWithTag+0x1a23ad:
fffff801`62ad2f5d 90              nop
@r15             Handle = 0x00000000`000024b0//handle address
ffff9903`d62c68c8 DesiredAccess = 1
@rbx             ObjectType = 0xffffe684`0f8b09e0
ffff9903`d62c68d8 AccessMode = 0n0 ''//kernel mode
ffff9903`d62c68e0 Tag = 0x746c6644
@r12             Object = 0xffff9903`d62c6940
ffff9903`d62c68f0 HandleInformation = 0x00000000`00000000
@r13             ObjectInfo = 0x00000000`00000000
<unavailable>     ObjectHeader = <value unavailable>
ffff9903`d62c6860 ObjectEntryData = union _HANDLE_TABLE_ENTRY
ffff9903`d62c68c0 Process = 0xffffe684`1fa57580
ffff9903`d62c68e8 ReleaseTable = 0x00 ''
@r14             Thread = 0xffffe684`1cf4f080
<unavailable>     ExtraInfo = <value unavailable>
<unavailable>     GrantedAccess = <value unavailable>
<unavailable>     HandleTable = <value unavailable>
<unavailable>     AuditOnClose = <value unavailable>
<unavailable>     Status = <value unavailable>
```

之后，我们看下 ObReferenceObjectByHandle 函数的具体用法及信息，参见以下链接：
https://docs.microsoft.com/en-us/windows-hardware/drivers/ddi/wdm/nf-wdm-obreferenceobjectbyhandle?redirectedfrom=MSDN

可以看到，问题是由于系统 Referencing user handle as KernelMode 导致，即 ObReferenceObjectByHandle 引用参数 AccessMode 为 kernelMode 下的 user handle，这是操作系统不允许的，进而造成的 C4 蓝屏。



无法显示链接的图像。该文件可能已被移动、重命名或删除。请验证该链接是否指向正确的文件和位置。

下一步动作：
=====================
建议联系 TMS 厂商进行问题排查，谢谢

李琦 Li Qi
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 Email: liqi@cmgos.com

发件人: Li Qi <liqi@cmgos.com>
发送时间: 2020年8月18日 18:34
收件人: 吴毓杰 <win10sup@sdc.icbc.com.cn>
抄送: Li Qi <liqi@cmgos.com>
主题: [案例号: CAS-02811-T4V2H7] % |P3|ICBC|插拔U盘设备时电脑蓝屏 % 初次响应 CMIT:0001729

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 李琦 。 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-02811-T4V2H7 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**”。

转载此邮件信息。任何第三方均不得查阅或使用此邮件信息。若您误收到本邮件，敬请及时通知发件人，并将邮件从您系统中彻底删除。发件人及中国工商银行均不对因邮件可能引发的损失负责。

This message is intended only for use of the addressees and any comment, statement or data contained herein is for the reference of the receivers only. Notification may not be sent for any revising related. Please do not disclose, copy, or distribute this e-mail without ICBC written permission. Any third party shall not read or use the content of this e-mail. If you receive this e-mail in error, please notify the sender immediately and delete this e-mail from your computer system completely.The sender and ICBC are not responsible for the loss caused possibly by e-mail.