陈先生，您好：

请参见以往邮件内容。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

发件人: Li Qi
发送时间: 2023 年 5 月 23 日 10:40
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-08913-W2T9D5] % |P2|ICBC|永丰分行登录系统异常 % 初次响应 CMIT:0001191

许先生，您好：

有关永丰分行的无法启动问题，目前对现场收集的 P2V 文件已经分析完成，具体请参见如下内容：

Case No：CAS-08913-W2T9D5

问题描述：

==========

用户反馈永丰分行一台电脑无法登录系统，北清路支行一台电脑发生蓝屏问题。

问题分析：

==========

1. 用户反馈开机出现“自动修复”问题，在关闭“自动修复”后，开机过程出现报错，无法找到 c:\windows\system32\config\system 文件，由于 system 文件是系统注册表文件，必须在启动过程中进行加载，未找到此文件则无法完成系统启动。
2. 进入 WinPE 查看，发现 c:\windows\system32\config 文件夹不存在，协助用户拷贝同版本系统的文件夹进行替换后，开机过程出现“0xc000000f”的报错，意为仍然缺少文件。遂抓取 P2V 进行分析。

```
C:\Users\liqi>err 0xc000000f
# for hex 0xc000000f / decimal -1073741809
  ISCSI_ERR_INVALID_CHAP_CHALLENGE                                iscsi
# CHAP challenge given by the target contains invalid
# characters. Dump data contains the challenge given.
  STATUS_NO_SUCH_FILE                                             ntsta
# {File Not Found}
# The file %hs does not exist.
  USBD_STATUS_NOT_ACCESSED                                        usb.h
# as an HRESULT: Severity: FAILURE (1), FACILITY_NULL (0x0), Code 0xf
```

3. 经 P2V 文件分析，在对系统盘进行磁盘操作的过程中发现 disk corruption，进行 chkdsk /f /r c:发现错误并完成修复。

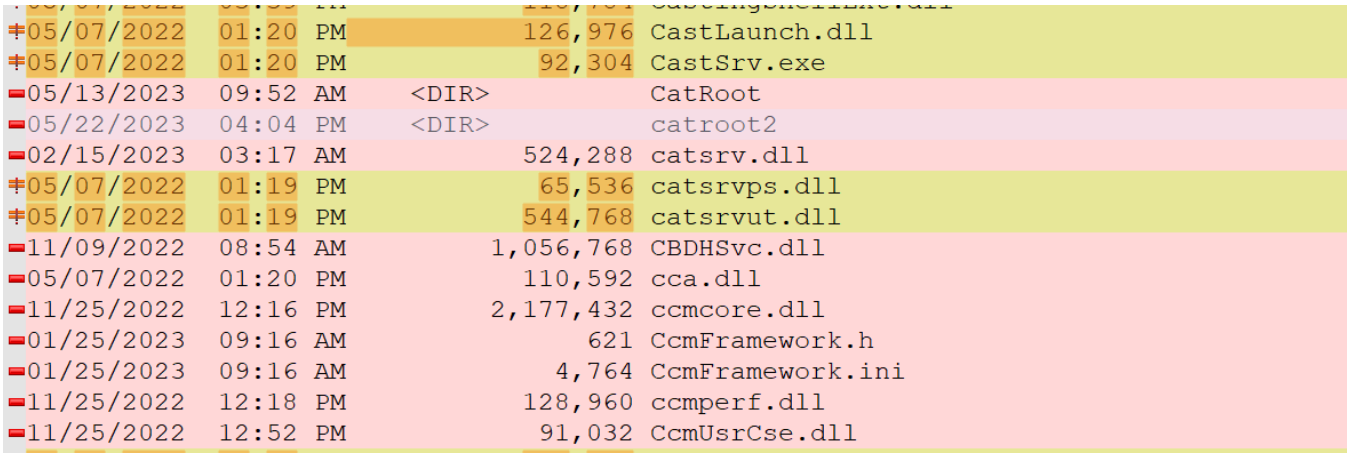
```
DISKPART> sel vol 1

Volume 1 is the selected volume.

DISKPART> shrink desired=200

Virtual Disk Service error:
The volume you have selected to shrink may be corrupted.
Use Chkdsk to fix the corruption problem, and then try to shrink the
volume again.
```

4. 问题依旧，经过与正常操作系统对 C 盘文件对比，发现缺失过多系统文件，如 catroot 文件夹也已经丢失，里面存放的是驱动签名文件。



```
05/07/2022  01:20 PM           126,976 CastLaunch.dll
05/07/2022  01:20 PM            92,304 CastSrv.exe
05/13/2023  09:52 AM    <DIR>          CatRoot
05/22/2023  04:04 PM    <DIR>          catroot2
02/15/2023  03:17 AM           524,288 catsrv.dll
05/07/2022  01:19 PM            65,536 catsrvps.dll
05/07/2022  01:19 PM           544,768 catsrvut.dll
11/09/2022  08:54 AM         1,056,768 CBDHSvc.dll
05/07/2022  01:20 PM           110,592 cca.dll
11/25/2022  12:16 PM         2,177,432 ccmcore.dll
01/25/2023  09:16 AM               621 CcmFramework.h
01/25/2023  09:16 AM             4,764 CcmFramework.ini
11/25/2022  12:18 PM           128,960 ccmperf.dll
11/25/2022  12:52 PM            91,032 CcmUsrCse.dll
```

结论：大量系统文件丢失，导致无法启动操作系统，建议重装系统。

问题总结：

==========

结合之前邮件内容，以上，为本次案例中所发生问题的全部内容，由于当前用户并未上报其他问题，相关问题电脑已做重装处理或无法再对上述问题进行复现，故此 case 将暂做归档处理，请您知悉，谢谢。如上述永丰分行或北清路支行的问题电脑再出现此问题，可随时与我联系，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

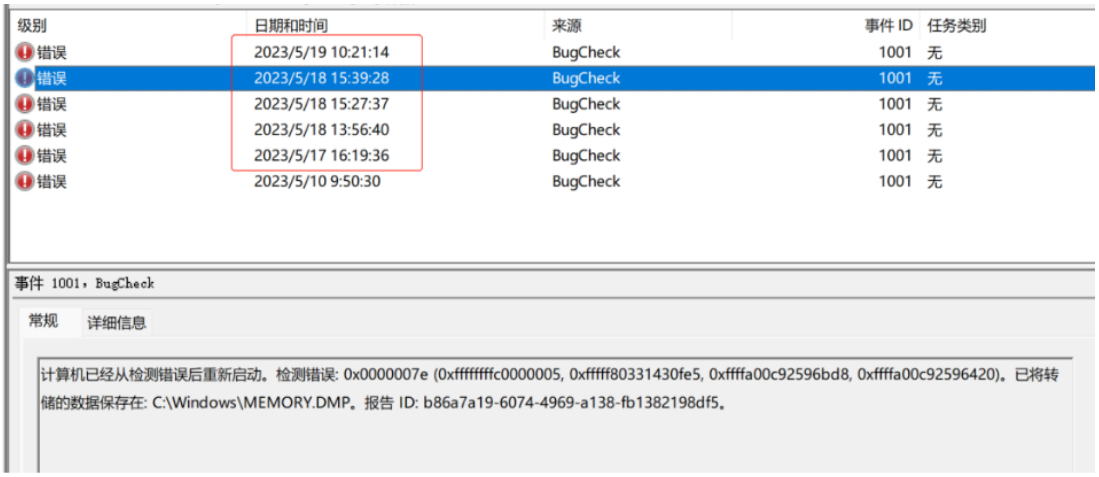
发件人: Li Qi
发送时间: 2023 年 5 月 22 日 15:11
收件人: 许翔 <win10sup@sdc.icbc.com.cn>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>

主题: 回复: [案例号: CAS-08913-W2T9D5] % |P2|ICBC|永丰分行登录系统异常 % 初次响应 CMIT:0001191

许先生，您好:

针对北清路支行上报的蓝屏问题目前已分析完毕，具体原因如下:

问题电脑发生的蓝屏均为 0x7e 的蓝屏问题，其中参数 1 是 0xc0000005 代表内存访问冲突。



级别	日期和时间	来源	事件 ID	任务类别
错误	2023/5/19 10:21:14	BugCheck	1001	无
错误	2023/5/18 15:39:28	BugCheck	1001	无
错误	2023/5/18 15:27:37	BugCheck	1001	无
错误	2023/5/18 13:56:40	BugCheck	1001	无
错误	2023/5/17 16:19:36	BugCheck	1001	无
错误	2023/5/10 9:50:30	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: 0x0000007e (0xffffffffc0000005, 0xfffff80331430fe5, 0xffffa00c92596bd8, 0xffffa00c92596420)。已将转储的数据保存在: C:\Windows\MEMORY.DMP。报告 ID: b86a7a19-6074-4969-a138-fb1382198df5。

查看 callstack，具体内存冲突地址段发生在 ftdibus 总线的运行阶段

```
Child-SP          RetAddr           : Args to Child                                                   : Call Site
fffff600`5717dbb8 ffff800`391e8bc6  : 00000000`0000007e ffffffff`c0000005 fffff800`39041fe5 fffff600`5717ebd8 : nt!KeBugCheckEx
fffff600`5717dbc0 ffff800`391a70ff  : fffdf0d`00000003 fffff600`5717fb10 fffff600`57179000 fffff600`57180000 : nt!PspSystemThreadStartup$filt$0+0x44
fffff600`5717dc00 ffff800`391d81df  : fffff600`5717fb10 fffff600`5717ele0 fffff600`5717e2c0 00000000`0010001f : nt!_C_specific_handler+0x9f
fffff600`5717dc70 ffff800`39094990  : fffff600`5717e2c0 00000000`00000000 fffff600`5717ele0 00000000`00000000 : nt!RtlpExecuteHandlerForException+0xf
fffff600`5717dca0 ffff800`39096c94  : fffff600`5717ebd8 fffff600`5717e920 fffff600`5717ebd8 ffffdf0d`0f800000 : nt!RtlDispatchException+0x430
fffff600`5717e3f0 ffff800`391e1902  : 00000000`00000000 fffff600`5717ec80 00000000`00001000 00000000`00000043 : nt!KiDispatchException+0x144
fffff600`5717eaa0 ffff800`391dd4e8  : fffff600`00000204 00000000`fffff600 00000000`20206f49 ffffdf0d`0f6c0010 : nt!KiExceptionDispatch+0xc2
fffff600`5717ec80 ffff800`39041fe5  : fffdf0d`0f800000 00000000`fffff600 00000000`00000000 fffff600`5717eea0 : nt!KiPageFault+0x428 (TrapFrame @ ffff
fffff600`5717ee10 ffff800`53c6a436  : fffdf0d`0f66a1a0 00000000`00000004 ffffdf0d`0f66a1e0 00000000`00000000 : nt!IofCallDriver+0x15
fffff600`5717ee50 ffff800`53c6a026  : 00000000`00000000 ffffdf0d`03d6bec0 00000000`00000000 ffffdf0d`03db1ce0 : ftdibus+0xa436
fffff600`5717ef40 ffff800`53c6a468  : fffff600`5717f0f0 00000000`00000000 ffffdf0d`0f66a1e0 00000000`00000008 : ftdibus+0xa026
fffff600`5717f0a0 ffff800`53c6a026  : 00000000`00000000 ffffdf0d`0c65bf80 00000000`00000000 00000000`00000000 : ftdibus+0xa468
fffff600`5717f190 ffff800`53c69bbc  : fffdf0d`0f66a1a0 00000000`00000000 ffffdf0d`0f66a1a0 00000000`00000000 : ftdibus+0xa026
fffff600`5717f2f0 ffff800`53c61ce5  : 00000000`00000000 00000000`00000000 00000000`00000000 ffffdf0d`0f66aafa : ftdibus+0x9bbc
fffff600`5717f400 ffff800`53c6163b  : 00000000`00000000 00000000`00000000 ffffdf0d`0f66a050 ffffdf0d`0f66a1a0 : ftdibus+0x1ce5
fffff600`5717f580 ffff800`53c6126b  : fffdf0d`0f69d7e0 fffff600`5717f760 fffdf0d`0f66a050 00000000`00000000 : ftdibus+0x163b
fffff600`5717f610 ffff800`39042029  : fffff600`5717f760 fffff800`3902cc23 00000000`00000017 00000000`69706e00 : ftdibus+0x126b
fffff600`5717f640 ffff800`3970f3de  : fffdf0d`0f3f5de0 fffdf0d`0f47c840 00000000`00000001 00000000`00000000 : nt!IofCallDriver+0x59
fffff600`5717f680 ffff800`3902b735  : fffdf0d`0f3f5de0 00000000`00000000 ffffdf0d`0f47c840 ffffdf0d`0f47c840 : nt!PnpAsynchronousCall+0xea
fffff600`5717f6c0 ffff800`3916e8c8  : 00000000`00000000 ffffdf0d`0f3f5de0 fffff800`3916df50 fffff800`3916df50 : nt!PnpSendIrp+0x95
fffff600`5717f730 ffff800`39701297  : fffdf0d`0c5e5c10 ffffdf0d`0f47c840 00000000`00000000 ffffdf0d`0c5e5c10 : nt!PnpStartDevice+0x88
fffff600`5717f7c0 ffff800`3970147f  : fffdf0d`0c5e5c10 00000000`00000000 00000000`00000001 fffff800`3916e42a : nt!PnpStartDeviceNode+0xdb
fffff600`5717f850 ffff800`396fc098  : fffdf0d`0c5e5c10 fffff600`5717f918 00000000`00000002 00000000`00000001 : nt!PipProcessStartPhase1+0x6f
fffff600`5717f8a0 ffff800`3971241a  : fffdf0d`0db68b00 fffff800`3903d101 fffff600`5717f9b0 ffffdf0d`00000002 : nt!PipProcessDevNodeTree+0x3dc
fffff600`5717f960 ffff800`3916f68d  : fffdf01`00000003 ffffdf0d`072b4c50 ffffdf0d`0db68b50 00000000`00000000 : nt!PiProcessReenumeration+0x82
fffff600`5717f9b0 ffff800`390c649a  : fffdf0d`0c502080 fffff800`39447460 ffffdf0d`042a54f0 ffffdf0d`00000000 : nt!PnpDeviceActionWorker+0x1dd
fffff600`5717fa70 ffff800`391481d5  : ffffdf0d`0c502080 ffffdf0d`042a4300 ffffdf0d`0c502080 000024ed`bd9bbfff : nt!ExpWorkerThread+0x16a
fffff600`5717fb10 ffff800`391d68dc  : ffffca00`c6b79180 ffffdf0d`0c502080 fffff800`39148180 00000000`00000000 : nt!PspSystemThreadStartup+0x55
fffff600`5717fb60 00000000`00000000  : fffff600`57180000 fffff600`57179000 00000000`00000000 00000000`00000000 : nt!KiStartSystemThread+0x1c
```

这是一个串口设备的总线模块，进一步查看其为 usb 设备，查看有问题的设备节点信息如下:

```
10: kd> !devnode ffffdf0d8c5e5c10
DevNode 0xffffdf0d8c5e5c10 for PDO 0xffffdf0d8f3f5de0
  Parent 0xffffdf0d8f5e8670   Sibling 0xffffdf0d870b58e0   Child 0000000000
  InstancePath is "USB\VID_0403&PID_6001\AH02P89L"
  ServiceName is "FTDIBUS"
  State = DeviceNodeStartPending (0x305)
  Previous State = DeviceNodeResourcesAssigned (0x304)
  StateHistory[03] = DeviceNodeResourcesAssigned (0x304)
  StateHistory[02] = DeviceNodeDriversAdded (0x303)
  StateHistory[01] = DeviceNodeInitialized (0x302)
  StateHistory[00] = DeviceNodeUninitialized (0x301)
  StateHistory[19] = Unknown State (0x0)
  StateHistory[18] = Unknown State (0x0)
  StateHistory[17] = Unknown State (0x0)
  StateHistory[16] = Unknown State (0x0)
  StateHistory[15] = Unknown State (0x0)
  StateHistory[14] = Unknown State (0x0)
  StateHistory[13] = Unknown State (0x0)
  StateHistory[12] = Unknown State (0x0)
  StateHistory[11] = Unknown State (0x0)
  StateHistory[10] = Unknown State (0x0)
  StateHistory[09] = Unknown State (0x0)
  StateHistory[08] = Unknown State (0x0)
  StateHistory[07] = Unknown State (0x0)
  StateHistory[06] = Unknown State (0x0)
  StateHistory[05] = Unknown State (0x0)
  StateHistory[04] = Unknown State (0x0)
  Flags (0x64000130)  DNF_ENUMERATED, DNF_IDS_QUERIED,
                      DNF_NO_RESOURCE_REQUIRED, DNF_NO_LOWER_DEVICE_FILTERS,
                      DNF_NO_UPPER_DEVICE_FILTERS, DNF_NO_UPPER_CLASS_FILTERS
  CapabilityFlags (0x00001c53)  DeviceD1, DeviceD2,
                                Removable, UniqueID,
                                WakeFromD0, WakeFromD1,
                                WakeFromD2
```

查看该硬件 ID 对应为 FT232 USB-Serial (UART) IC 的芯片，设备序列号应为 AH02P89L，可以请现场用户确认一下是否存在该设备。由于当前问题暂不复现，请在上述检查完后，移除对应设备继续观察，如再次出现蓝屏问题，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 <liqi@cmgos.com>
发送时间: 2023 年 5 月 12 日 9:45
收件人: 许翔 <win10sup@sdc.icbc.com.cn>

抄送: Li Qi <liqi@cmgos.com>
主题: [案例号: CAS-08913-W2T9D5] % |P2|ICBC|永丰分行登录系统异常 % 初次响应 CMIT:0001191

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 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-08913-W2T9D5 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
