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 14:36
主题: 回复: [案例号: CAS-02814-D7K8Z9] % |P3|ICBC|使用设备频繁蓝屏 % 初次响应 CMIT:0001731

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-02814-D7K8Z9] % |P3|ICBC|使用设备频繁蓝屏 % 初次响应 CMIT:0001731

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-02814-D7K8Z9

问题描述:
==========
用户反馈，正常使用设备频繁蓝屏

问题分析:
==========
魏女士的电脑频繁蓝屏问题，分析结果与一年前的 TMS 问题类似，结果如下:
系统 crash 是由于 list entry 出现损坏导致
Bugcheck 信息:
Bugcheck details
==========
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: ffffe28054c37200, Address of the trap frame for the exception that caused the bugcheck
Arg3: ffffe28054c37158, Address of the exception record for the exception that caused the bugcheck
Arg4: 0000000000000000, Reserved

Crashing Stack
==========
Process Thread CID UserTime KernelTime ContextSwitches Wait Reason Time State
System (ffffbc8523e62200) ffffbc8535046040 4.2080 0s 9s.328 362906 Executive 0s Running on CPU 0

Call stack 信息:
0 ffffe28054c36ed8 fffff80357fd88e9 nt!KeBugCheckEx+0x0
1 ffffe28054c36ee0 fffff80357fd8c90 nt!KiBugCheckDispatch+0x69
2 ffffe28054c37020 fffff80357fd708e nt!KiFastFailDispatch+0xd0
3 ffffe28054c37200 fffff803583ba457 nt!KiRaiseSecurityCheckFailure+0x30e
4 (Inline) ---------- nt!RtlFailFast+0x5
5 (Inline) ---------- nt!FatalListEntryError+0x5
6 (Inline) ---------- nt!RemoveHeadList+0x65
7 ffffe28054c37390 fffff8035b4f953f nt!FsRtlTeardownPerFileContexts+0xc7

在进行 remove head list 时发生 crash，损坏的地址为：
损坏的地址为 0xffffbc85`33f67d10
0: kd> .frame 0n6;dv /t /v
06 (Inline Function) --------`-------- nt!RemoveHeadList+0x65
[internal\minwin\priv_sdk\inc\ntrtl_x.h @ 900]

@rsi struct _LIST_ENTRY * Entry = 0xffffbc85`33f67d10 [ 0xffffbc85`33f4b108 - 0x00000000`00000000]
@rax struct _LIST_ENTRY * NextEntry = 0xffffbc85`33f4b108 [ 0xffffbc85`33f67d08 - 0xffffbc85`33f67d08]

0: kd> dx -id 0,0,ffffbc8523e62200 -r1 ((ntkrnlmp!_LIST_ENTRY *)0xffffbc8533f67d10)
((ntkrnlmp!_LIST_ENTRY *)0xffffbc8533f67d10) : 0xffffbc8533f67d10 [Type: _LIST_ENTRY *]
[+0x000] Flink : 0xffffbc8533f4b108 [Type: _LIST_ENTRY *]
[+0x008] Blink : 0x0 [Type: _LIST_ENTRY *]
查看这个 list entry 的 pool 分布信息，发现在这个 pool 的 block 之前是 tag 为 Filt 的 block，即 vwifimf.sys。大概率怀疑是 Filt 越界写导致的。
ffffbc8533f67c00 size: 30 previous size: 0 (Allocated) FSfc
ffffbc8533f67c30 size: 30 previous size: 0 (Allocated) FSfc
ffffbc8533f67c60 size: 30 previous size: 0 (Allocated) FOCX
ffffbc8533f67c90 size: 30 previous size: 0 (Allocated) Io
ffffbc8533f67cc0 size: 30 previous size: 0 (Allocated) Filt
*ffffbc8533f67cf0 size: 30 previous size: 0 (Allocated) *FSfc
Pooltag FSfc : Unrecoginzed File System Run Time allocations (update pooltag.w), Binary : nt!fsrtl
ffffbc8533f67d20 size: 30 previous size: 0 (Free) FSfc

下一步动作:
==========
由于无法开启 special pool，故而无法进一步定位到 TMS 具体的读写操作过程。建议由 TMS 厂商进行进一步排查，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 18:37
收件人: 吴毓杰 <win10sup@sdc.icbc.com.cn>
抄送: Li Qi <liqi@cmgos.com>
主题: [案例号: CAS-02814-D7K8Z9] % |P3|ICBC|使用设备频繁蓝屏 % 初次响应 CMIT:0001731

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-02814-D7K8Z9 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”。