

毓杰，您好：

如刚才电话沟通，目前针对吴总的 dump 的分析已完成，已找到发生蓝屏问题的原因，经您同意，此 case 将暂做关闭处理，以下为案例总结，请您知悉：

Case No：CAS-02905-W7N4D4

问题描述：

=====

CMGE 在远程办公时蓝屏。

问题分析：

=====

此次蓝屏的原因是由于 list entry 损坏导致，具体由谁引起，需要深入分析后给出结论。该问题与当前正在分析中的 vwifmf 在重组网络数据包过程中传参错误导致蓝瓶的问题不同，因此经客户同意后，暂不做深入分析。以下为该 dump 的分析信息：

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: fffffc01541ff710, Address of the trap frame for the exception that caused the bugcheck

Arg3: fffffc01541ff668, Address of the exception record for the exception that caused the bugcheck

Arg4: 0000000000000000, Reserved

```

NOTE: The trap frame does not contain all registers.
Some register values may be zeroed or incorrect.
rax=ffffa7833ee51f00 rbx=0000000000000000 rcx=0000000000000003
rdx=ffffa7834439eb00 rsi=0000000000000000 rdi=0000000000000000
rip=fffff80718a29d9b rsp=fffffc01541ff8a0 rbp=fffffc01541ffa00
r8=fffffc01541ff8a8 r9=0000000000000000 r10=ffffa7834514080
r11=fffffc01541ff840 r12=0000000000000000 r13=0000000000000000
r14=0000000000000000 r15=0000000000000000
iopl=0         nv up ei ng nz na po cy
nt!EtwpReceiveNotification+0x1d8917:
fffff80718a29d9b cd29             int     29h
Resetting default scope

EXCEPTION_RECORD: fffffc01541ff668 -- (.exr 0xfffffc01541ff668)
ExceptionAddress: fffff80718a29d9b (nt!EtwpReceiveNotification+0x000000000001d8917)
ExceptionCode: c0000409 (Security check failure or stack buffer overrun)
ExceptionFlags: 00000001
NumberParameters: 1
  Parameter[0]: 0000000000000003
Subcode: 0x3 FAST_FAIL_CORRUPT_LIST_ENTRY

```

问题总结:

=====

结合工行现场之前蓝屏问题的分析结论, 请优先协调 TMS 处理, 明确出现 list entry 错误的问题场景, 并给出相应的解决方案。具体可参见附件邮件内容。

经与用户沟通, 目前完成此 dump 的分析工作, 同意关闭此 case。

以上, 如您后续有任何问题, 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.

服务电话: 4008180055

电子邮箱 Email: [liqi@cmgos.com](mailto:liqi@cmgos.com)



发件人: Li Qi <[liqi@cmgos.com](mailto:liqi@cmgos.com)>

发送时间: 2020 年 9 月 4 日 13:43

收件人: 吴毓杰 <[win10sup@sdicbc.com.cn](mailto:win10sup@sdicbc.com.cn)>

抄送: Li Qi <[liqi@cmgos.com](mailto:liqi@cmgos.com)>

主题: [案例号: CAS-02905-W7N4D4 ] % |P3|CBC|领导使用神州网信政府版系统的电脑在远程办公时蓝屏 % 初次响应 CMIT:0001956

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-02905-W7N4D4 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”。