Hi，徐达：

感谢您的回复,鉴于目前未收到客户更新的反馈意见，经您的同意，此 case 将暂做归档处理，后续有任何问题，可再重启此 case 进行跟踪。以下为案例总结，请您知悉

Case No：CAS-01825-D2H2W7

问题描述：
==========
用户反馈自动化跑长时间 S5 压力测试，过程中出现 BSOD 现象

问题分析：
==========
经过对 dump 文件分析，该问题已在最新补丁中得以修复。具体原因已在此前邮件向用户解释

问题总结：

==========

建议用户安装最新补丁 KB4520062。鉴于目前未收到客户更新的反馈意见，经同意，此 case 将暂做归档处理，后续有任何问题，可再重启此 case 进行跟踪。

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: Xu Da <xuda@cmgos.com>
发送时间: 2020 年 2 月 24 日 10:04
收件人: Li Qi <liqi@cmgos.com>
抄送: CRM Case Email <casemail@cmgos.com>; Liu Jian <liujian@cmgos.com>; Xu Da <xuda@cmgos.com>
主题: 答复: [案例号：CAS-01825-D2H2W7]％ | P3 | Lenovo | 客户测试导入 V2020-L，S5 出现 BSOD ％初次响应 CMIT:0001081

Hi Liqi,

客户方面之前 confirm 的反馈时间已经过了，这个问题请先 Close，如果客户有进一步反馈再另外开 Case，多谢

发件人: Xu Da
发送时间: Tuesday, February 11, 2020 9:55 AM
收件人: Li Qi <liqi@cmgos.com>
抄送: CRM Case Email <casemail@cmgos.com>; Liu Jian <liujian@cmgos.com>; Xu Da <xuda@cmgos.com>
主题: 回复: [案例号: CAS-01825-D2H2W7] % | P3 | Lenovo | 客户测试导入 V2020-L，S5 出现 BSOD % 初次响应 CMIT:0001081

Hi Liqi,
谢谢回复，已同客户沟通测试，等客户测试结果出来后再讨论后续行动。

发件人: Li Qi <liqi@cmgos.com>
发送时间: 2020 年 2 月 11 日 9:31
收件人: Xu Da <xuda@cmgos.com>
抄送: CRM Case Email <casemail@cmgos.com>; Liu Jian <liujian@cmgos.com>
主题: 回复: [案例号: CAS-01825-D2H2W7] % | P3 | Lenovo | 客户测试导入 V2020-L，S5 出现 BSOD % 初次响应 CMIT:0001081

Hi，徐达：

目前已完成对 dump 文件的分析，以下是分析结果：

1．有关 0x3B，系统访问无效的内存地址导致的问题。

```
SYSTEM_SERVICE_EXCEPTION (3b)
An exception happened while executing a system service routine.
Arguments:
Arg1: 00000000c0000005, Exception code that caused the bugcheck
Arg2: fffff80111624f6f, Address of the instruction which caused the bugcheck
Arg3: fffff88f785dea80, Address of the context record for the exception that caused the bugcheck
Arg4: 0000000000000000, zero.
```

2．crash 的 call stack 如下，可以看到问题发生的时候，正在做 wlan 相关的操作。直接原因是 sid 的值不对。

```
7: kd> !mex.t
Process                                  Thread        CID      UserTime KernelTime
ContextSwitches Wait Reason Time State
svchost.exe (LocalSystemNetworkRestricted) (ffffca0c884f6240) ffffca0c88525080
c84.ca8      16ms       0s          138 Executive     0s Running on CPU 7

# Child-SP        Return          Call Site
 0 fffff88f785de148 fffff801111dd8e9 nt!KeBugCheckEx+0x0
```

```
 1 fffff88f785de150 fffff801111dcd3c nt!KiBugCheckDispatch+0x69
 2 fffff88f785de290 fffff801111d4b5f nt!KiSystemServiceHandler+0x7c
 3 fffff88f785de2d0 fffff8011112d450 nt!RtlpExecuteHandlerForException+0xf
 4 fffff88f785de300 fffff8011103ac24 nt!RtlDispatchException+0x430
 5 fffff88f785dea50 fffff801111dd9c2 nt!KiDispatchException+0x144
 6 fffff88f785df100 fffff801111d984b nt!KiExceptionDispatch+0xc2
 7 fffff88f785df2e0 fffff80111624f6f nt!KiGeneralProtectionFault+0x30b
 8 fffff88f785df478 fffff801116206ea nt!RtlValidSid+0xf
 9 fffff88f785df480 fffff8011187b23a nt!RtlValidSecurityDescriptor+0x8a
 a fffff88f785df4b0 fffff801117b7a3f nt!ObpSetObjectAuditInfo+0x2a
...............................................................................
17 000000b0b51fec30 00007fff4b992f4f
WLANMSM!Dot11MsmAdaptInit+0xb7
18 000000b0b51fec70 00007fff4ba8d758
WLANMSM!Dot11MsmInitAdapter+0x8f
19 000000b0b51fecc0 00007fff4ba6a36c wlansvc!IntfInitContext+0x35c
1a 000000b0b51ff470 00007fff4ba6b53e wlansvc!WimAddInterface+0x3b8
1b 000000b0b51ff5d0 00007fff4ba6b728
wlansvc!WimRnwfDeviceEventHandler+0x376
1c 000000b0b51ff670 00007fff4ba70488
wlansvc!WimNotificationHandler+0x120
1d 000000b0b51ff6e0 00007fff618e21c5
wlansvc!NhWrkDeviceNotificationHandler+0x108
1e 000000b0b51ff750 00007fff618c05c4 ntdll!RtlpTpWorkCallback+0x165
1f 000000b0b51ff830 00007fff60677974 ntdll!TppWorkerThread+0x644
20 000000b0b51ffb20 00007fff618da271
KERNEL32!BaseThreadInitThunk+0x14
21 000000b0b51ffb50 0000000000000000 ntdll!RtlUserThreadStart+0x21

7: kd> .frame /r 0x8; !mex.x
08 fffff88f`785df478 fffff801`116206ea nt!RtlValidSid+0xf [minkernel\ntos\rtl\sertl.c @ 1135]
rax=00007fffffff0000 rbx=ffffda8fc4553c70 rcx=005c006500630069
rdx=fffff88f785df608 rsi=fffff88f785df608 rdi=0000000000000736
rip=fffff80111624f6f rsp=fffff88f785df478 rbp=ffffca0c89302d10
r8=0000000000000000  r9=000000000000000f r10=ffffca0c7d466b20
r11=fffff88f785df410 r12=ca0c89302d100001 r13=ffffca0c89302d10
r14=ffffca0c894ea000 r15=ffffda8fc4553c70
iopl=0         nv up ei ng nz na po nc
cs=0010  ss=0018  ds=002b  es=002b  fs=0053  gs=002b             efl=00000286
nt!RtlValidSid+0xf:
fffff801`11624f6f 0fb601          movzx   eax,byte ptr [rcx] ds:002b:005c0065`00630069=??
@rcx            Sid = 0x005c0065`00630069

7: kd> !pte 0x005c0065`00630069
                                           VA 005c006500630069
PXE at FFFF95CAE572B000    PPE at FFFF95CAE5600CA0    PDE at FFFF95CAC0194018    PTE at
FFFF958032803180
contains 0A0000013DBAB867  contains 0000000000000000
```

```
pfn 13dbab    ---DA--UWEV  contains 0000000000000000
not valid

WARNING: noncanonical VA, accesses will fault !
```

由于 NT 当时访问了无效的内存地址，抛出 access violation 的异常，触发蓝屏.
关于 SID 地址异常的情况,发现是由于代码问题导致该数据没有被正确的初始化. 因而导致后面在 valid SID 地址的时候出现访问违规问题导致蓝屏

3. 当前使用的 wifi 驱动如下：

```
7: kd> dx -r1 ((WLANMSM!_DOT11_ADAPTER *)0xb0b51ff060)
((WLANMSM!_DOT11_ADAPTER *)0xb0b51ff060)                 : 0xb0b51ff060 [Type: _DOT11_ADAPTER *]
    [+0x000] gAdapterId       : {6A7CF4CD-AC11-4CC2-8317-C877EF15FF5D} [Type: _GUID]
    [+0x010] pszDescription   : 0x239746750c0 : "Microsoft Wi-Fi Direct Virtual Adapter" [Type: wchar_t *]
    [+0x018] Dot11CurrentOpMode [Type: _DOT11_CURRENT_OPERATION_MODE]
```

4. 检查当前系统的系统补丁，安装到 KB4516077

```
* 10.0.17763.771 | ntoskrnl.exe | 4516077 | 2019/09/24      | 2019.09 C - Cumulative Non-Security (Update) for Windows 10 1809
```

5. 针对此问题，目前可以确认，需要修复系统组件 nwifi，因此请安装 KB4520062

以上，请用户在进行测试之前先安装 KB4520062，然后再对问题进行复现，看是否可以解决此问题。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 1 月 17 日 9:38
收件人: Xu Da <xuda@cmgos.com>
抄送: CRM Case Email <casemail@cmgos.com>; Liu Jian <liujian@cmgos.com>

主题: 回复: [案例号: CAS-01825-D2H2W7] % | P3 | Lenovo | 客户测试导入 V2020-L, S5 出现 BSOD % 初次响应 CMIT:0001081

Hi, 徐达:

根据您的需求，我谨在此问题涉及的范围定义:

问题范围: 用户反馈自动化跑长时间 S5 压力测试，过程中出现 BSOD 现象

问题定义: 协助用户分析处理此问题

如您对以上问题范围定义有任何疑问请直接与我联系。

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 1 月 17 日 9:31
收件人: Xu Da <xuda@cmgos.com>
抄送: Li Qi <liqi@cmgos.com>
主题: [案例号: CAS-01825-D2H2W7] % | P3 | Lenovo | 客户测试导入 V2020-L, S5 出现 BSOD % 初次响应 CMIT:0001081

徐达 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-01825-D2H2W7 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**”。