Hi Guannan,

情况已了解，我们会向 Lenovo 反馈。

Best Regards,

Monica Gao Meng（高矇）

发件人: Shi Guannan <shign@cmgos.com>
发送时间: 2023 年 2 月 20 日 15:22
收件人: Jia Wei <jiawei@cmgos.com>; Gao Meng <gaomeng@cmgos.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: 回复: [案例号: CAS-07480-N2N2L8] % | P3 | Lenovo| V2022-L 测试中发现重启存在蓝屏 % 初次响应 CMIT:0001859

Hi Gaomeng,

Sophie 在与 PG team 沟通后，PG team 仍然拒绝了修复此问题，拒绝原因如下:

- 问题复现概低 - only 15% repro rate; only occurs after reboot
- 当前有可行的 workaround - disable Lenovo Intelligent sensing
- Business Justification 不够 – 此问题并不仅在 CMGE 发生，建议联想尝试通过 OEM channel 直接升级到微软，以提高 Business Justification

另外 Sophie 对此问题仍存在些疑问:
It seems that this is also not a regression and has existed in the code for some time. Did Lenovo not originally test the Intelligent Sense feature on Win10 21H2 and similar platforms with the same codebase (Win10 20H1 and beyond)?
If this issue is truly critical to Lenovo, why wouldn't they be willing to directly engage with Microsoft?

如果需要 Sophie 继续跟进此问题还需提供 Sophie 需要的信息。谢谢!

Best,
石冠男 Shi Guannan
Customer Support Operation Advisor
C&M Information Technologies Co.,Ltd.
手机 Mobile: +86 15901008883
电子邮箱 Email: shign@cmgos.com

神州网信
CMIT

发件人: Jia Wei <jiawei@cmgos.com>
发送时间: 2023 年 2 月 2 日 15:03
收件人: Gao Meng <gaomeng@cmgos.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: 回复: [案例号: CAS-07480-N2N2L8] ％ | P3 | Lenovo| V2022-L 测试中发现重启存在蓝屏 ％ 初次响应 CMIT:0001859

Hi Gao Meng,

根据 MS CSS 工程师的反馈，总结对于此问题的答复如下：

- 技术层面上，从日志中没有看到中国政府版的定制组件或工作逻辑；
- 同时在其内部案例库中确实有相同的案例，且问题设备并未安装神州网信系统。

基于上述两点，**MS 方面认为这个问题应该与中国政府版定制系统无关，为系统底层组件的处理逻辑问题。**

- 神州网信方面提供了多次 Business Impact，MS CSS 根据日志分析也推测底层组件的处理逻辑存在异常，所有的信息已全部提交给 PG 团队。
- 但由于 MS CSS 团队负责的是实际商业生产应用中，设备在使用微软产品时遇到的问题。目前 PG 团队在查看完 MS CSS 团队提交的信息后，因其不符合"in market"的标准，不满足 Business Impact 的定义，无法进行产品层面的查看或修复。
- 同时 MS CSS 团队经过内部咨询确认**当前场景确实超过 CSS 团队的负责范畴，建议协同厂商走 OEM Partner 渠道**。该渠道有别于 CSS 渠道，可以处理 OEM 场景下微软系统与硬件厂商的技术问题，并得到 OEM 产品组的支持。

贾伟 Jia Wei
神州网信技术有限公司
服务支持电话： 400-818-0055
电子邮箱： jiawei@cmgos.com

C&M Information Technologies Co., Ltd.
11F, Block C North Building, Raycom InfoTech Park, Beijing
mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人: Jia Wei
发送时间: 2023 年 2 月 1 日 10:47
收件人: Gao Meng <gaomeng@cmgos.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: 回复: [案例号: CAS-07480-N2N2L8] % | P3 | Lenovo| V2022-L 测试中发现重启存在蓝屏 % 初次响应 CMIT:0001859

Hi Gao Meng,

我已将最新 Impact 提交，并电话沟通再次强调问题严重性，催促问题跟进。

如有进展将随时更新。

贾伟 Jia Wei
神州网信技术有限公司
服务支持电话： 400-818-0055
电子邮箱： jiawei@cmgos.com

C&M Information Technologies Co., Ltd.
11F, Block C North Building, Raycom InfoTech Park, Beijing
mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人: Jia Wei
发送时间: 2023 年 1 月 31 日 16:57
收件人: Gao Meng <gaomeng@cmgos.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: 回复: [案例号: CAS-07480-N2N2L8] % | P3 | Lenovo| V2022-L 测试中发现重启存在蓝屏 % 初次响应 CMIT:0001859

Hi Gao Meng,

收到，我会尽快将最新 Impact 信息更新并与相关人员沟通、推进案例。

贾伟 Jia Wei
神州网信技术有限公司
服务支持电话： 400-818-0055
电子邮箱： jiawei@cmgos.com

C&M Information Technologies Co., Ltd.
11F, Block C North Building, Raycom InfoTech Park, Beijing

mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人: Gao Meng <gaomeng@cmgos.com>
发送时间: 2023 年 1 月 31 日 16:55
收件人: Jia Wei <jiawei@cmgos.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: 回复: [案例号: CAS-07480-N2N2L8] % | P3 | Lenovo| V2022-L 测试中发现重启存在蓝屏 % 初次响应 CMIT:0001859

Hi Jiawei,

我们希望能够有关此问题的积极更新。
此问题会影响接下来 OEM 联想在 V2022-L 的持续出货，根据影响的机型平台等情况分析有可能导致超过 150k 无法出货且将影响部分大客户（如：工行、招行等）的投标，还请尽快提供进一步的分析情况及解决方案。

Best Regards,

Monica Gao Meng（高曚）

发件人: Jia Wei <jiawei@cmgos.com>
发送时间: 2022 年 12 月 7 日 15:48
收件人: Gao Meng <gaomeng@cmgos.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: 回复: [案例号: CAS-07480-N2N2L8] % | P3 | Lenovo| V2022-L 测试中发现重启存在蓝屏 % 初次响应 CMIT:0001859

Hi Gao Meng

目前此问题已经提交 MS，但经过沟通仍未得到进一步反馈信息。

Bug ID 见之前沟通内容，如果最终用户希望尽快得到结果，也可以通过其他渠道推进。

贾伟 Jia Wei
神州网信技术有限公司
服务支持电话： 400-818-0055
电子邮箱： jiawei@cmgos.com

C&M Information Technologies Co., Ltd.
11F, Block C North Building, Raycom InfoTech Park, Beijing
mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人: Gao Meng <gaomeng@cmgos.com>
发送时间: 2022 年 12 月 7 日 14:34
收件人: Jia Wei <jiawei@cmgos.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: 回复: [案例号: CAS-07480-N2N2L8] % | P3 | Lenovo| V2022-L 测试中发现重启存在蓝屏 % 初次响应 CMIT:0001859

Hi Jiawei,

是否有进一步的更新?

Best Regards,

Monica Gao Meng（高曚）

发件人: Jia Wei <jiawei@cmgos.com>
发送时间: 2022 年 11 月 23 日 10:42
收件人: Gao Meng <gaomeng@cmgos.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: 回复: [案例号: CAS-07480-N2N2L8] % | P3 | Lenovo| V2022-L 测试中发现重启存在蓝屏 % 初次响应 CMIT:0001859

好的，收到

贾伟 Jia Wei
神州网信技术有限公司
服务支持电话： 400-818-0055
电子邮箱： jiawei@cmgos.com

C&M Information Technologies Co., Ltd.
11F, Block C North Building, Raycom InfoTech Park, Beijing
mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人: Gao Meng <gaomeng@cmgos.com>
发送时间: 2022 年 11 月 23 日 10:40
收件人: Jia Wei <jiawei@cmgos.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: 回复: [案例号: CAS-07480-N2N2L8] % | P3 | Lenovo| V2022-L 测试中发现重启存在蓝屏 % 初次响应 CMIT:0001859

Update BI

Business Impact

The Business Impact will be used and read by many people that are not familiar with the technology in question. It will be presented in one or more shiprooms and discussed in terms of impact generically and contrasted with other bugs. We need to understand the impact of this issue in a non-technical manner. This lets us evaluate issues apples to apples and assures that we are applying resources to the right problems.
Be sure that your problem description and impact below contains details on the following.

How many users/machines are impacted? (And out of how many?)	BSOD happen on Lenovo Thinkpad brand . 2500 impacted machines have been shipped, and, 2 projects, more than 50 thousands of machines block because of this issue.
Is this a "Mission Critical" system? (Y/N)	Y
How Long has this issue been affecting the customer?	5 months

Describe the Customer Scenario in detail:

For users, they will meet such BSOD after shutdown at unexpected time points. CMGE users are all government users. The appearance of this issues will affect users' work and even affect users' trust in our products.

How often is the customer impacted by this issue? *(We want to know the frequency the customer is impacted. If the problem is 100% reproducible then how often is the scenario performed?)*

NA

Describe the day to day impact of this issue non-technically (Try to explain it in terms or dollars, hours or capabilities):

The BSOD issue will not often occur on the user’s machine, but once it occurs, it will make bad user impact

What changed to trigger this issue?

After install Lenovo Intelligent sensing, BSOD appear

What will the customer do if this bug is not fixed?

Complain to OEM

Please describe the customer’ s business timeline associated with this fix

Need to fix it before 22/12/01

If Windows is being used to deliver a product or a service to a 3rd party, please describe it. Also, please be sure to mention if the product/service is not yet available:

NA

Best Regards,

Monica Gao Meng（高曚）

发件人: Jia Wei <jiawei@cmgos.com>
发送时间: 2022 年 11 月 23 日 10:30
收件人: Gao Meng <gaomeng@cmgos.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: 回复: [案例号: CAS-07480-N2N2L8] % | P3 | Lenovo| V2022-L 测试中发现重启存在蓝屏 % 初次响应 CMIT:0001859

Hi Gao Meng,

关于此案例的最新分析更新：

When WUDFHost.exe tries to create file object, it sends a IRP_MJ_QUERY_SECURITY irp to the device object, IopGetSetSecurityObject() does not do anything about the irp->IoStatus.Status field. So, chances are that it is set to 0 (STATUS_SUCCESS). STATUS_SUCCESS is returned, but ACPI.SYS hasn't touched irp->UserBuffer either, so when it contains an invalid memory address, the system bugchecks when the stack later uses that address as PSECURITY_DESCRIPTOR.

//Checking the crash information. The directly issue is the rax value 8290c617`dcfe6443 is invalid.

```
10: kd> !mex.t ffffc48af2ac30c0
Process                    Thread          CID       UserTime KernelTime ContextSwitches COM-
Init                 Wait Reason Time State
WUDFHost.exe (ffffc48af2c4d0c0) ffffc48af2ac30c0
644.660        0s        0s              5  APTKIND_MULTITHREADED (MTA) UserRequest   0s
Running on CPU 10

Priority:
    Current Base UB FB IO Page
    13      8    80 80 2  5

# Child-SP         Return           Call Site                        Info
 0 ffffd48de3201268 fffff8054960a869 nt!KeBugCheckEx+0x0
 1 ffffd48de3201270 fffff80549609cbc nt!KiBugCheckDispatch+0x69
 2 ffffd48de32013b0 fffff805496017b2 nt!KiSystemServiceHandler+0x7c
 3 ffffd48de32013f0 fffff805494e2467 nt!RtlpExecuteHandlerForException+0x12
 4 ffffd48de3201420 fffff805494e1066 nt!RtlDispatchException+0x297
 5 ffffd48de3201b40 fffff8054960a9ac nt!KiDispatchException+0x186
 6 ffffd48de3202200 fffff805496066e0 nt!KiExceptionDispatch+0x12c
 7 ffffd48de32023e0 fffff805497f8acf nt!KiGeneralProtectionFault+0x320
 8 ffffd48de3202578 fffff805498e4901 nt!RtlValidSid+0xf
 9 ffffd48de3202580 fffff80549adab52 nt!RtlValidSecurityDescriptor+0x81
 a ffffd48de32025b0 fffff80549825cfb nt!ObpSetObjectAuditInfo+0x2a
 b ffffd48de32025e0 fffff80549801e5f nt!ObpCreateHandle+0x10fb
 c ffffd48de32027f0 fffff80549888f0f nt!ObOpenObjectByNameEx+0x31f
 d ffffd48de3202920 fffff80549888ae9 nt!IopCreateFile+0x40f
 e ffffd48de32029c0 fffff8054960a2b8 nt!NtCreateFile+0x79
 f ffffd48de3202a50 00007ffcc10ad9e4 nt!KiSystemServiceCopyEnd+0x28
10 00000023c9bfecd8 00007ffcbedca070 ntdll!ZwCreateFile+0x14
11 00000023c9bfece0 00007ffcbedc9d96 KERNELBASE!CreateFileInternal+0x2c0
12 00000023c9bfee40 00007ff74e4d9475 KERNELBASE!CreateFileW+0x66
13 00000023c9bfeea0 00007ff74e4f047b
WUDFHost!CWudfDeviceStack::Initialize+0xa6d
```

```
14 00000023c9bfef90 00007ff74e4cbc56
WUDFHost!CLpcNotification::InitializeDeviceStack+0x167
15 00000023c9bff0a0 00007ffcbd5051f2
WUDFHost!CLpcNotification::Message+0x14a6
16 00000023c9bff350 00007ffcbd50440e
WUDFPlatform!WdfLpcPort::ProcessMessage+0x122
17 00000023c9bff410 00007ffcbd50612f
WUDFPlatform!WdfLpcCommPort::ProcessMessage+0x8e
18 00000023c9bff460 00007ffcbd507e5e
WUDFPlatform!WdfLpcConnPort::ProcessMessage+0xef
19 00000023c9bff510 00007ff74e4d3f80
WUDFPlatform!WdfLpc::RetrieveMessage+0x15e
1a (Inline)        ----------------
WUDFHost!CThreadpool::WorkerThread+0x4a
1b 00000023c9bff680 00007ffcc1020ebc WUDFHost!ThreadPoolWorkerThunk+0x50
1c 00000023c9bff6b0 00007ffcc1062f26 ntdll!TppExecuteWaitCallback+0xa4
1d 00000023c9bff700 00007ffcc0b37034 ntdll!TppWorkerThread+0x456
1e 00000023c9bffa00 00007ffcc1062651 KERNEL32!BaseThreadInitThunk+0x14
1f 00000023c9bffa30 0000000000000000 ntdll!RtlUserThreadStart+0x21
```

This thread is crashing.

```
10: kd> .frame /r 0x8;.echo;!mex.x
08 ffffd48d`e3202578 fffff805`498e4901 nt!RtlValidSid+0xf
rax=00007ffffff0000 rbx=ffffd80d0be7fd70 rcx=8290c617dcfe6443
rdx=ffffd48de3202720 rsi=ffffd48de3202720 rdi=0000000000000722
rip=fffff805497f8acf rsp=ffffd48de3202578 rbp=ffffc48af50f85a0
r8=0000000000000000  r9=00000000000001f0 r10=ffffc48ae11ebdc0
r11=ffffd48de3202510 r12=ffffc48af50f85a0 r13=0000000000000400
r14=ffffd80d0be7fd00 r15=0000000000000000
iopl=0         nv up ei ng nz na pe nc
cs=0010  ss=0018  ds=002b  es=002b  fs=0053  gs=002b             efl=00040282
nt!RtlValidSid+0xf:
fffff805`497f8acf 0fb601          movzx   eax,byte ptr [rcx] ds:002b:8290c617`dcfe6443=??

@rcx             Sid = 0x8290c617`dcfe6443
```

//Check the irp processing, the trigger is “ACPI\ACPI0008\5&239f155b&0”, a Light Sensor.

```
10: kd> .frame /r 0xb;.echo;!mex.x
0b ffffd48d`e32025e0 fffff805`49801e5f nt!ObpCreateHandle+0x10fb
rax=00007ffffff0000 rbx=000000000000028c rcx=8290c617dcfe6443
rdx=ffffd48de3202720 rsi=ffffc48ae72e1010 rdi=0000000000000000
```

```
rip=fffff80549825cfb rsp=ffffd48de32025e0 rbp=ffffd48de3202700
r8=0000000000000000  r9=00000000000001f0 r10=ffffc48ae11ebdc0
r11=ffffd48de3202510 r12=ffffc48af50f85a0 r13=0000000000000400
r14=ffffd80d0be7fd70 r15=0000000000000000
iopl=0         nv up ei ng nz na pe nc
cs=0010  ss=0018  ds=002b  es=002b  fs=0053  gs=002b             efl=00040282
nt!ObpCreateHandle+0x10fb:
fffff805`49825cfb eb10            jmp     nt!ObpCreateHandle+0x110d (fffff805`49825d0d)

ffffd48d`e32026e0 OpenReason = ObCreateHandle (0n0)
ffffd48d`e3202690 Object = 0xffffc48a`f50f85d0

10: kd> !mex.fo 0xffffc48a`f50f85d0
File Details: ffffc48af50f85d0

   Name                                             Device           Driver           Vpb Flags Byte
Offset       FsContext       FsContext2 Owning Process
   =====================================================
================ ================ ====== ===== ===========
================ ================ ===============
   \WudfElevation-08f48bc6-2e61-11ed-bf4d-a8934ad623a4 ffffc48aeed02c90
\Driver\WudfRd (null)     0          0 0000000000000000 0000000000000000

10: kd> !mex.deviceobject ffffc48aeed02c90
Device          : ffffc48aeed02c90
Driver          : ffffc48aee18fe30
Name            : \Driver\WudfRd
Current Irp     :
Ref             : 1
Type            : 32: FILE_DEVICE_ACPI
Flags           :
Dacl            : ffffd80d07c77160
Device Extension: ffffc48aeed02de0
DevObj Extension: ffffc48aeed02e08
Dope            :
Device Node     :
Ext Flags       : 0: None

10: kd> !mex.ddt nt!_DEVICE_OBJECT ffffc48aeed02c90

dt nt!_DEVICE_OBJECT ffffc48aeed02c90 () Recursive: [ -r1 -r2 -r ] Verbose Normal dt
============================================================
========================
   +0x000 Type                    : 0n3
   +0x002 Size                    : 0x178 (0n376)
   +0x004 ReferenceCount          : 0n1
   +0x008 DriverObject            : 0xffffc48a`ee18fe30 _DRIVER_OBJECT
   +0x010 NextDevice              : 0xffffc48a`eeb8ed20
_DEVICE_OBJECT   !deviceobject   !devstack
   +0x018 AttachedDevice          : (null)
   +0x020 CurrentIrp              : (null)
   +0x028 Timer                   : (null)
   +0x030 Flags                   : 0x40 = DO_DEVICE_HAS_NAME
   +0x034 Characteristics         : 0x180 = FILE_AUTOGENERATED_DEVICE_NAME,
FILE_DEVICE_SECURE_OPEN
   +0x038 Vpb                     : (null)
   +0x040 DeviceExtension         : 0xffffc48a`eed02de0 Void    [ !ndao dps dc !handle ln ? ]
   +0x048 DeviceType              : 0x32 = FILE_DEVICE_ACPI
   +0x04c StackSize               : 4 ''
   +0x050 Queue                   : <anonymous-tag>
   +0x098 AlignmentRequirement    : 0
   +0x0a0 DeviceQueue             : _KDEVICE_QUEUE
   +0x0c8 Dpc                     : _KDPC
   +0x108 ActiveThreadCount       : 0
   +0x110 SecurityDescriptor      : 0xffffd80d`07c77160 Void  [security descriptor]
   +0x118 DeviceLock              : _KEVENT
   +0x130 SectorSize              : 0
   +0x132 Spare1                  : 0
   +0x138 DeviceObjectExtension   : 0xffffc48a`eed02e08 _DEVOBJ_EXTENSION
   +0x140 Reserved                : (null)

10: kd> !devstack 0xffffc48a`eeb8ed20
  !DevObj           !DrvObj            !DevExt           ObjectName
> ffffc48aeeb8ed20  \Driver\WudfRd     ffffc48aeeb8ee70
  ffffc48aeeb98db0  \Driver\acpials    ffffc48aeeb98ce0
  ffffc48ae31c4060  \Driver\ACPI       ffffc48ae30b3010  00000043
!DevNode ffffc48ae31c6050 :
  DeviceInst is "ACPI\ACPI0008\5&239f155b&0"
  ServiceName is "SensorsAlsDriver"

ACPI\ACPI0008\5&239f155b&0        Light Sensor                    ffffc48ae31c6050
SensorsAlsD.. WUDFRd.sys       0x303 0x00     0x00        ***            acpials
```

贾伟 Jia Wei

神州网信技术有限公司
服务支持电话： 400-818-0055
电子邮箱： jiawei@cmgos.com

C&M Information Technologies Co., Ltd.
11F, Block C North Building, Raycom InfoTech Park, Beijing
mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人: Gao Meng <gaomeng@cmgos.com>
发送时间: 2022 年 11 月 23 日 10:23
收件人: Jia Wei <jiawei@cmgos.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: 回复: [案例号: CAS-07480-N2N2L8]％ | P3 | Lenovo| V2022-L 测试中发现重启存在蓝屏 ％初次响应 CMIT:0001859

Hi Jiawei,

目前 Bug 是否有新的进展，客户 Lenovo 希望能尽快得到更新。

Best Regards,

Monica Gao Meng（高曚）

发件人: Gao Meng
发送时间: 2022 年 11 月 11 日 8:46
收件人: Jia Wei <jiawei@cmgos.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: 回复: [案例号: CAS-07480-N2N2L8]％ | P3 | Lenovo| V2022-L 测试中发现重启存在蓝屏 ％初次响应 CMIT:0001859

Hi Jiawei,

以下为联想提供的 Business Impact:

Business Impact

The Business Impact will be used and read by many people that are not familiar with the technology in question. It will be presented in one or more shiprooms and discussed in terms of impact generically and contrasted with other bugs. We need to understand the impact of this issue in a non-technical manner. This lets us

evaluate issues apples to apples and assures that we are applying resources to the right problems.
Be sure that your problem description and impact below contains details on the following.

How many users/machines are impacted? (And out of how many?)	BSOD happen on Lenovo Thinkpad brand . 2500 impacted machines have been shipped, and, 2 projects, thousands of machines block because of this issue.
Is this a "Mission Critical" system? (Y/N)	Y
How Long has this issue been affecting the customer?	5 months

Describe the Customer Scenario in detail:

For users,they will meet such BSOD after shutdown at unexpected time points. CMGE users are all government users. The appearance of this issues will affect users' work and even affect users' trust in our products.

How often is the customer impacted by this issue? *(We want to know the frequency the customer is impacted. If the problem is 100% reproducible then how often is the scenario performed?)*

NA

Describe the day to day impact of this issue non-technically (Try to explain it in terms or dollars, hours or capabilities):

The BSOD issue will not often occur on the user's machine, but once it occurs, it will make bad user impact

What changed to trigger this issue?

After install Lenovo Intelligent sensing，BSOD appear

What will the customer do if this bug is not fixed?

Complain to OEM

Please describe the customer’s business timeline associated with this fix

Need to fix it before 22/12/01

If Windows is being used to deliver a product or a service to a 3rd party, please describe it. Also, please be sure to mention if the product/service is not yet available:

NA

Best Regards,

Monica Gao Meng（高曚）

发件人: Jia Wei <jiawei@cmgos.com>
发送时间: 2022年11月10日 9:41
收件人: Gao Meng <gaomeng@cmgos.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: 回复: [案例号: CAS-07480-N2N2L8]％ | P3 | Lenovo| V2022-L 测试中发现重启存在蓝屏 ％初次响应 CMIT:0001859

Hi Gao Meng,

以下是抓取 Verifier.exe 后生成 Dump 的分析过程，请查看：

问题发生在我们去验证 object 的 sid 之后，返回了一个 invalid 的值所以触发了 bugcheck

```
00 ffffd48d`e3201268 fffff805`4960a869     nt!KeBugCheckEx
01 ffffd48d`e3201270 fffff805`49609cbc     nt!KiBugCheckDispatch+0x69
02 ffffd48d`e32013b0 fffff805`496017b2     nt!KiSystemServiceHandler+0x7c
03 ffffd48d`e32013f0
fffff805`494e2467     nt!RtlpExecuteHandlerForException+0x12
04 ffffd48d`e3201420 fffff805`494e1066     nt!RtlDispatchException+0x297
05 ffffd48d`e3201b40 fffff805`4960a9ac     nt!KiDispatchException+0x186
```

```
06 ffffd48d`e3202200 fffff805`496066e0     nt!KiExceptionDispatch+0x12c
07 ffffd48d`e32023e0 fffff805`497f8acf     nt!KiGeneralProtectionFault+0x320
08 ffffd48d`e3202578 fffff805`498e4901     nt!RtlValidSid+0xf
09 ffffd48d`e3202580 fffff805`49adab52     nt!RtlValidSecurityDescriptor+0x81
0a ffffd48d`e32025b0 fffff805`49825cfb     nt!ObpSetObjectAuditInfo+0x2a
0b ffffd48d`e32025e0 fffff805`49801e5f     nt!ObpCreateHandle+0x10fb
0c ffffd48d`e32027f0 fffff805`49888f0f     nt!ObOpenObjectByNameEx+0x31f
0d ffffd48d`e3202920 fffff805`49888ae9     nt!IopCreateFile+0x40f
0e ffffd48d`e32029c0 fffff805`4960a2b8     nt!NtCreateFile+0x79
0f ffffd48d`e3202a50 00007ffc`c10ad9e4     nt!KiSystemServiceCopyEnd+0x28
10 00000023`c9bfecd8 00000000`00000000     ntdll!ZwCreateFile+0x14
```

// 往前查看我们创建的 file object，WUDFHost.exe 尝试去 create file object，它发送了一个 irp 给 device object，往前找该对应的 device 就是 SensorsAlsDriver

```
10: kd> .frame 0n11;dv /t /v
0b ffffd48d`e32025e0 fffff805`49801e5f     nt!ObpCreateHandle+0x10fb
ffffd48d`e32026e0 _OB_OPEN_REASON OpenReason = ObCreateHandle (0n0)
ffffd48d`e3202690 void * Object = 0xffffc48a`f50f85d0
ffffd48d`e32026b8 unsigned long DesiredAccess = 0


10: kd> !fileobject 0xffffc48a`f50f85d0
File Details: ffffc48af50f85d0
    Name                                                Device           Driver
           Vpb Flags Byte Offset        FsContext       FsContext2 Owning
Process
    ===================================================  ================
============== ====== ===== =========== ================ ================
==============
    \WudfElevation-08f48bc6-2e61-11ed-bf4d-a8934ad623a4  ffffc48aeed02c90
\Driver\WudfRd (null)     0           0 0000000000000000 0000000000000000

10: kd> !devstack ffffc48aeed02c90
  !DevObj           !DrvObj            !DevExt           ObjectName
> ffffc48aeed02c90  \Driver\WudfRd     ffffc48aeed02de0  UMDFCtrlDev-08f48bc5-
2e61-11ed-bf4d-a8934ad623a4

10: kd> !ddt WUDFRd!_DEVICE_EXTENSION ffffc48aeed02de0
dt WUDFRd!_DEVICE_EXTENSION ffffc48aeed02de0 () Recursive: [ -r1 -r2 -r ]
Verbose Normal dt
================================================================================
==
   +0x000 RdDevice                 : ffffc48a`f5783220 RdDevice [Derived class
is RdCtrlDevice @ ffffc48a`f5783220]
   +0x008 RemoveLock               :  IO REMOVE LOCK

10: kd> !mex.ddt ffffc48a`f5783220 WUDFRd!RdDevice
dt ffffc48a`f5783220 WUDFRd!RdDevice () Recursive: [ -r1 -r2 -r ] Verbose Normal
dt
================================================================================
==
[Derived class is RdCtrlDevice @ ffffc48a`f5783220] [View original type]
   +0x010 m_ConstructorStatus      : 0n0
   +0x020 m_Lock                   : WUDF LOCK
   +0x000 __VFN_table              : 0xfffff805`aca2d5e0
   +0x008 m_RefCount               : 1
   +0x028 m_Parent                 : ffffc48a`f56de490 WdfObject [Derived class
is WdfObjectList<RdCtrlDevice,RdCtrlDeviceParameters> @ ffffc48a`f56de490]
```

```
   +0x030 m_Next                    : ffffc48a`f57669d0 WdfObject [Derived class
is RdCtrlDevice @ ffffc48a`f57669d0]
   +0x038 m_UniqueObjectId          : 2
   +0x03c m_DeleteWaitInAction      : 0 ''
   +0x040 m_Event                   : WUDF_EVENT
   +0x048 m_Name                    : 0xffffc48a`f5778c10 "UMDFCtrlDev-08f48bc5-
2e61-11ed-bf4d-a8934ad623a4"
   +0x050 m_MarkedForDelete         : 0 ''
   +0x051 m_ObjectType              : 11 ( RdTypeControlDownDevice )
   +0x058 m_DosDeviceName           : _UNICODE_STRING  "\DosDevices\UMDFCtrlDev-
08f48bc5-2e61-11ed-bf4d-a8934ad623a4" = "\DosDevices\UMDFCtrlDev-08f48bc5-2e61-
11ed-bf4d-a8934ad623a4"
   +0x068 m_DeviceObject            : 0xffffc48a`eed02c90
_DEVICE_OBJECT   !deviceobject   !devstack
   +0x070 m_NextLowerDeviceObject   : 0xffffc48a`eeb98db0
_DEVICE_OBJECT   !deviceobject   !devstack

10: kd> !devstack 0xffffc48a`eeb98db0
  !DevObj           !DrvObj            !DevExt           ObjectName
  ffffc48aeeb8ed20  \Driver\WudfRd     ffffc48aeeb8ee70
> ffffc48aeeb98db0  \Driver\acpials    ffffc48aeeb98ce0
  ffffc48ae31c4060  \Driver\ACPI       ffffc48ae30b3010  00000043
!DevNode ffffc48ae31c6050 :
  DeviceInst is "ACPI\ACPI0008\5&239f155b&0"
  ServiceName is "SensorsAlsDriver"
```

```
---------------------------------------------------------------------------------------------------
```

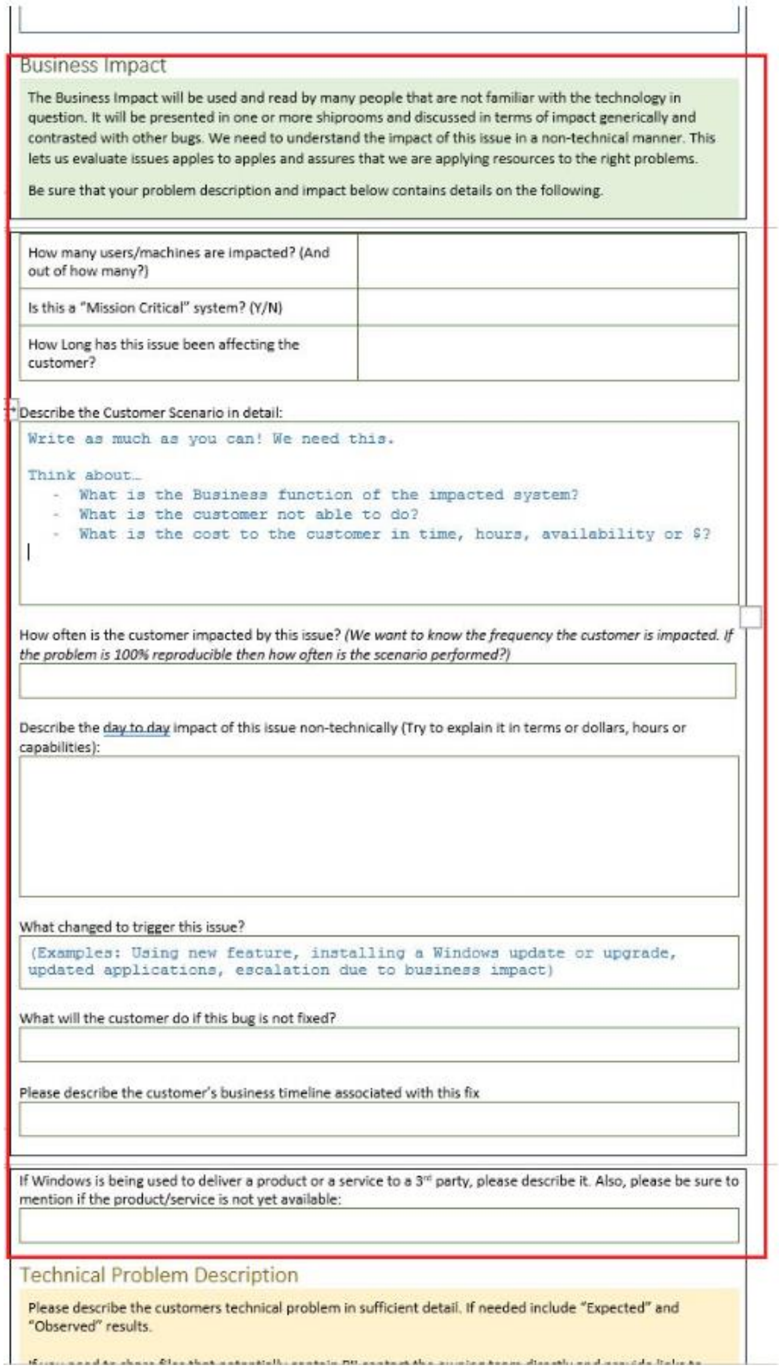
贾伟 Jia Wei
神州网信技术有限公司
服务支持电话： 400-818-0055
电子邮箱： jiawei@cmgos.com

C&M Information Technologies Co., Ltd.
11F, Block C North Building, Raycom InfoTech Park, Beijing
mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人: Jia Wei
发送时间: 2022 年 11 月 8 日 11:09
收件人: Gao Meng <gaomeng@cmgos.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: 回复: [案例号: CAS-07480-N2N2L8] % | P3 | Lenovo| V2022-L 测试中发现重启存在蓝屏 % 初次响应 CMIT:0001859

高女士，您好

关于问题升级处理，还需要协助提供附件中关于"Business Impact"部分。



Business Impact

The Business Impact will be used and read by many people that are not familiar with the technology in question. It will be presented in one or more shiprooms and discussed in terms of impact generically and contrasted with other bugs. We need to understand the impact of this issue in a non-technical manner. This lets us evaluate issues apples to apples and assures that we are applying resources to the right problems.

Be sure that your problem description and impact below contains details on the following.

How many users/machines are impacted? (And out of how many?)	
Is this a "Mission Critical" system? (Y/N)	
How Long has this issue been affecting the customer?	

Describe the Customer Scenario in detail:

```
Write as much as you can! We need this.

Think about…
   -  What is the Business function of the impacted system?
   -  What is the customer not able to do?
   -  What is the cost to the customer in time, hours, availability or $?
```

How often is the customer impacted by this issue? *(We want to know the frequency the customer is impacted. If the problem is 100% reproducible then how often is the scenario performed?)*

Describe the day to day impact of this issue non-technically (Try to explain it in terms or dollars, hours or capabilities):

What changed to trigger this issue?

```
(Examples: Using new feature, installing a Windows update or upgrade,
updated applications, escalation due to business impact)
```

What will the customer do if this bug is not fixed?

Please describe the customer's business timeline associated with this fix

If Windows is being used to deliver a product or a service to a 3rd party, please describe it. Also, please be sure to mention if the product/service is not yet available:

Technical Problem Description

Please describe the customers technical problem in sufficient detail. If needed include "Expected" and "Observed" results.

贾伟 Jia Wei
神州网信技术有限公司
服务支持电话： 400-818-0055
电子邮箱： jiawei@cmgos.com

C&M Information Technologies Co., Ltd.
11F, Block C North Building, Raycom InfoTech Park, Beijing
mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人: Jia Wei
发送时间: 2022 年 11 月 4 日 13:58
收件人: Gao Meng <gaomeng@cmgos.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: 回复: [案例号: CAS-07480-N2N2L8] % | P3 | Lenovo| V2022-L 测试中发现重启存在蓝屏 % 初次响应 CMIT:0001859

高女士，您好

当前收到的日志没有开启 special pool，建议按照下方方式开启 Special pool，按照附件方法配置后抓取 Full Dump。

```
0: kd> !verifier

Verify Flags Level 0x00000000

  STANDARD FLAGS:
    [ ] (0x00000000) Automatic Checks
    [ ] (0x00000001) Special pool
    [ ] (0x00000002) Force IRQL checking
    [ ] (0x00000008) Pool tracking
    [ ] (0x00000010) I/O verification
    [ ] (0x00000020) Deadlock detection
    [ ] (0x00000080) DMA checking
    [ ] (0x00000100) Security checks
    [ ] (0x00000800) Miscellaneous checks
    [ ] (0x00020000) DDI compliance checking

  ADDITIONAL FLAGS:
    [ ] (0x00000004) Randomized low resources simulation
    [ ] (0x00000200) Force pending I/O requests
    [ ] (0x00000400) IRP logging
    [ ] (0x00002000) Invariant MDL checking for stack
    [ ] (0x00004000) Invariant MDL checking for driver
    [ ] (0x00008000) Power framework delay fuzzing
    [ ] (0x00010000) Port/miniport interface checking
    [ ] (0x00040000) Systematic low resources simulation
    [ ] (0x00080000) DDI compliance checking (additional)
    [ ] (0x00200000) NDIS/WIFI verification
    [ ] (0x00800000) Kernel synchronization delay fuzzing
    [ ] (0x01000000) VM switch verification
    [ ] (0x02000000) Code integrity checks

    [X] Indicates flag is enabled
```

开启、关闭 Special pool:

1、开 special pool

请按照如下方法开启 special pool:

a. 右键单击开始按钮-> 选择“运行”, 输入 verifier 点击确认.

b. 选择 "创建自定义设置" 再点击下一步.

c. 勾选 "特殊池" 再点击下一步.

d. 选择“从一个列表选择驱动程序名”

e. 点击“全选”，再点击完成

f. 重启计算机生效

Important:

1. Enabling the Special Pool may impact the performance of the computer.

2. If the computer is unable to start up, please use "Last Known Good" to undo the changes made above:

-- Keep press F8 key until the Windows Startup menu appears.

-- Choose the "Last Known Good Configuration", and press Enter.

2. 关闭 special pool

a. 右键单击开始按钮-> 选择“运行”, 输入 verifier 点击确认.

b. 选择“删除现有设置”，点击完成，再重启生效

贾伟 Jia Wei
神州网信技术有限公司
服务支持电话：400-818-0055
电子邮箱：jiawei@cmgos.com

C&M Information Technologies Co., Ltd.
11F, Block C North Building, Raycom InfoTech Park, Beijing
mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人: Jia Wei <jiawei@cmgos.com>
发送时间: 2022 年 11 月 1 日 11:52
收件人: Gao Meng <gaomeng@cmgos.com>
抄送: Jia Wei <jiawei@cmgos.com>

主题: [案例号: CAS-07480-N2N2L8] % | P3 | Lenovo| V2022-L 测试中发现重启存在蓝屏 % 初次响应 CMIT:0001859

高曚 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 贾伟 。 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-07480-N2N2L8 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”。