谢谢!

发件人: Li Qi <liqi@cmgos.com>
发送时间: 2021 年 7 月 23 日 14:42
收件人: Liu Wei <liuwei@cmgos.com>
抄送: Case_Notification <Case_Notification@cmgos.com>
主题: 回复: [案例号: CAS-04505-J0K0K4] % 售前反馈需要协助分析兴业银行 dump 文件 % 初次响应 CMIT:0001456

Hi，刘伟:

如刚才线下沟通，目前用户暂无后续支持要求，此 case 经您同意，做关闭处理，以下为案例总结，请您知悉:

Case No：CAS-04505-J0K0K4

问题描述:

==========

用户反馈在插入安全 U 盘会蓝屏，协助分析蓝屏 dump。

问题分析:

==========

如之前 dump 分析，蓝屏原因为系统线程在执行错误处理程序时发生内存访问冲突导致。HID 在处理删除设备对象时引发的 pagefault。HID 类库属于 windows driver,在传输过程中会涉及到其他 module，因此也不排除其他三方 module 加载导致此问题。:

建议:
1， 系统补丁更新至最新版本
2， 硬件驱动更新至最新版本，尤其是 usb 驱动

如上述操作无效，则需要联系 TSM 厂商进行排查分析。

问题总结:

==========

经用户确认，目前用户暂无后续支持要求，此 case 将做关闭处理。

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.
服务支持电话： 4008180055
电子邮箱 Email: liqi@cmgos.com

发件人: Li Qi
发送时间: 2021 年 7 月 23 日 14:41
收件人: Liu Wei <liuwei@cmgos.com>
抄送: Case_Notification <Case_Notification@cmgos.com>
主题: 回复: [案例号: CAS-04505-J0K0K4] % 售前反馈需要协助分析兴业银行 dump 文件 % 初次响应 CMIT:0001456

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: 2021 年 7 月 20 日 16:56
收件人: Liu Wei <liuwei@cmgos.com>
抄送: Case_Notification <Case_Notification@cmgos.com>
主题: 回复: [案例号: CAS-04505-J0K0K4] % 售前反馈需要协助分析兴业银行 dump 文件 % 初次响应 CMIT:0001456

Hi, 刘伟:

我谨在此阐述我们双方针对这个问题所涉及范围界定:

问题定义:

用户反馈在插入安全 U 盘会蓝屏，协助分析蓝屏 dump

问题范围:

我们将协助您分析处理上述问题，并对定义的问题给予最大的技术支持。

如果能及时解决问题，或问题属于产品设计的行为，或问题涉及到三方，我们将考虑关闭案例。如果存在多个问题，则我们考虑拆分案例进行分析。

接下来，我们将开始合作解决这个问题。如果您对以上的问题范围界定有任何异议，请尽快告知。如果您有其他任何疑问。也欢迎随时与我联系。

从 dump 来看，有如下分析及建议：
Dump bugcheck 为 7e，系统线程在执行错误处理程序时发生内存访问冲突导致的蓝屏问题。
以下为部分 call stack 信息
fffff30f`6aaf11e8 fffff804`597e0a21 : 00000000`0000007e ffffffff`c0000005 fffff804`66ba2816 fffff30f`6aaf2208 : nt!KeBugCheckEx
fffff30f`6aaf11f0 fffff804`597a3552 : ffff988a`00000003 fffff30f`6aaf2c10 fffff30f`6aaed000 fffff30f`6aaf3000 : nt!PspSystemThreadStartup$filt$0+0x44
fffff30f`6aaf1230 fffff804`597d1b62 : fffff30f`6aaf2c10 fffff30f`6aaf1810 fffff30f`6aaf18f0 00000000`0010001f : nt!_C_specific_handler+0xa2
fffff30f`6aaf12a0 fffff804`5972a450 : fffff30f`6aaf18f0 00000000`00000000 fffff30f`6aaf1810 00000000`00000000 : nt!RtlpExecuteHandlerForException+0x12
fffff30f`6aaf12d0 fffff804`59637c24 : fffff30f`6aaf2208 fffff30f`6aaf1f50 fffff30f`6aaf2208 00000000`00000000 : nt!RtlDispatchException+0x430
fffff30f`6aaf1a20 fffff804`597da9c2 : 00000000`00001000 fffff30f`6aaf22b0 ffff8000`00000000 00000000`00000058 : nt!KiDispatchException+0x144
fffff30f`6aaf20d0 fffff804`597d6cae : ffff988a`00000000 ffff8785`00000001 ffff988a`77014000 ffff8785`6c1fee00 : nt!KiExceptionDispatch+0xc2
fffff30f`6aaf22b0 fffff804`66ba2816 : ffff988a`77010060 ffff988a`20206f49 ffff988a`00000808 00000000`43646948 : nt!KiPageFault+0x42e (TrapFrame @ fffff30f`6aaf22b0)
fffff30f`6aaf2440 fffff804`66ba330b : ffff988a`770101d0 ffff988a`77010408 ffff988a`79f529d0 ffff988a`770101d0 : HIDCLASS!HidpDeleteDeviceObjects+0x5a
fffff30f`6aaf2470 fffff804`66ba370a : 00000000`00000000 ffff988a`79f52900 ffff988a`77010408 ffff988a`79f529d0 : HIDCLASS!HidpCleanUpFdo+0x11b
fffff30f`6aaf24a0 fffff804`66ba0d24 : ffff988a`770101b0 ffff988a`79f52f20 ffff988a`79f529d0 00000000`00000002 : HIDCLASS!HidpRemoveDevice+0x1ba
fffff30f`6aaf24f0 fffff804`66b9b25a : ffff988a`770101b0 ffff988a`79f529d0 fffff804`66b8e638 00000000`00000001 : HIDCLASS!HidpFdoPnp+0x4ca4
fffff30f`6aaf2560 fffff804`66b71fe8 : ffff988a`770101d0 ffff988a`770101b0 ffff988a`7700dd00 00000000`00000011 : HIDCLASS!HidpIrpMajorPnp+0x6a
fffff30f`6aaf25a0 fffff804`5968db99 : ffff988a`77010060 00000000`00000000 ffff988a`79f529d0 00000000`69706e00 : HIDCLASS!HidpMajorHandler+0xe8

fffff30f`6aaf2630 fffff804`59c7253d : 00000000`00000000 ffff988a`77010060 fffff30f`6aaf2720 ffff988a`79f529d0 : nt!IofCallDriver+0x59
fffff30f`6aaf2670 fffff804`59cf0f39 : 00000000`00000002 fffff30f`6aaf2739 ffff988a`75edcbb0 ffff988a`7700dd00 : nt!IopSynchronousCall+0xe5
fffff30f`6aaf26e0 fffff804`5976b9cd : ffff8785`711de430 ffff988a`75edcbb0 00000000`0000000a ffff988a`7700dd00 : nt!IopRemoveDevice+0x105
从 call stack 中并未发现与三方应用有关，蓝屏原因为 HID 在处理删除设备对象时引发的 pagefault。HID 类库属于 windows driver,在传输过程中会涉及到其他 module，因此也不排除其他三方 module 加载导致此问题。
https://docs.microsoft.com/en-us/windows-hardware/drivers/hid/hid-architecture

vertarget
Windows 10 Kernel Version 17763 MP (4 procs) Free x64
Product: WinNt, suite: TerminalServer SingleUserTS
Built by: 17763.1.amd64fre.rs5_release.180914-1434
Machine Name:
Kernel base = 0xfffff804`59615000 PsLoadedModuleList = 0xfffff804`59a30670
Debug session time: Fri Jul 16 15:29:19.128 2021 (UTC + 8:00)
System Uptime: 0 days 0:02:41.982

!address fffff80466ba2816
Usage: Module
Base Address: fffff804`66b70000
End Address: fffff804`66bab000
Region Size: 00000000`0003b000
VA Type: BootLoaded
Module name: HIDCLASS.SYS
Module path: [\SystemRoot\System32\drivers\HIDCLASS.SYS]

User mode 下的加载 module 情况：

```
3: kd> !mex.mods nt -v
Number of modules: loaded: 175 unloaded: 5
```

Num	Base	End	Module name	Size kb	Checksum	Time stamp	CLR	Arch	Version	Bin Version	Product Version
1	fffff80459615000	fffff8045a085000	nt	10,688	0093e04d	015833E0	No	???	0.0.0.0	0.0.0.0	
10	fffff8045a511000	fffff8045a51d000	ntosext	48	00010f99	6D6B5A0E	No	???	0.0.0.0	0.0.0.0	
19	fffff80464070000	fffff8046408a000	SgrmAgent	104	00019298	F7CA286D	No	???	0.0.0.0	0.0.0.0	
22	fffff80464170000	fffff804641b3000	intelpep	268	0004a922	AE0E514F	No	???	0.0.0.0	0.0.0.0	
35	fffff80464470000	fffff8046448f000	mountmgr	124	000282fb	A8481DD2	No	???	0.0.0.0	0.0.0.0	
46	fffff804648d0000	fffff804648f0000	mcupdate_AuthenticAMD	128	00022a7f	F26DBE88	No	???	0.0.0.0	0.0.0.0	
54	fffff80464b10000	fffff80464d9d000	Ntfs	2,612	0028a9fa	3885B4CF	No	???	10.0.17763.592 (WinBuild.160101.0800)	10.0.17763.592	10.0.17763.592
80	fffff80465610000	fffff80465688000	fvevol	480	000809fb	204B6F56	No	???	0.0.0.0	0.0.0.0	
88	fffff80465a20000	fffff80465a2d580	TSMControl64	53	0001b8af	2015-03-19 01:51:01	No	???	0.0.0.0	0.0.0.0	
166	fffff8046a950000	fffff8046a95d000	WSDPrint	52	0000d12a	FBB4B133	No	???	0.0.0.0	0.0.0.0	

建议：
1， 系统补丁更新至最新版本
2， 硬件驱动更新至最新版本，尤其是 usb 驱动

如上述操作无效，则需要联系 TSM 厂商进行排查分析。

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: 2021 年 7 月 20 日 14:03
收件人: Liu Wei <liuwei@cmgos.com>
抄送: Li Qi <liqi@cmgos.com>
主题: [案例号: CAS-04505-J0K0K4] % 售前反馈需要协助分析兴业银行 dump 文件 % 初次响应 CMIT:0001456

刘伟 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-04505-J0K0K4 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
