张先生 您好:

感谢您的电话接听。

经过您的同意，我将暂时归档此案例。

工单的归档并不会影响我们为您提供技术支持服务，如有其他问题，您可以随时联系我们。

案例总结：

问题定义：

用户反馈中再保险有一台设备出现蓝屏问题，需要协助分析。

问题总结：

建议用户更新或卸载金格 KGChromePlugin 插件后，查看是否问题复现，并请三方应用厂商排查，暂时归档案例。

问题排查：

dump 文件显示 bugcheck 代码为 0xa（IRQL_NOT_LESS_OR_EQUAL），这个错误检查是由使用不适当地址的内核模式设备驱动程序引起的。这个错误检查表明，在提高中断请求级别（IRQL）时，有人试图访问一个无效的地址。其原因是一个坏的内存指针或设备驱动代码的 pageability 问题。

查看出问题时的 call stack 情况，显示 kgpm_64.sys 驱动 FAULTING_IP。kgpm_64.sys 文件位置为：C:\Program Files (x86)\KGChromPlugin\x64\kgpm_64.sys，为 2020 年 5 月版本。查询它是金格针对 Chrome 浏览器的插件，请三方应用厂商排查是否存在更新，如无使用必要，可进行卸载后再次观察，问题是否解决。

以上，如您后续有任何问题，可随时与我们联系，谢谢。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

发件人: Wei Liang
发送时间: 2023 年 6 月 26 日 17:39
收件人: 'yw_zhangzhe_o@chinare.com.cn' <yw_zhangzhe_o@chinare.com.cn>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: 回复: [案例号：CAS-09233-C4V1M3]％ TAM-中再保险用户反馈蓝屏问题 ％初次响应 CMIT:0001812

张先生 您好:

感谢您的电话接听。

根据您提供的信息，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:

用户反馈中再保险有一台设备出现蓝屏问题，需要协助分析。

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。

分析您提供的 dump 文件，显示由于 bugcheck 代码为 **0xa**（IRQL_NOT_LESS_OR_EQUAL），这个错误检查是由使用不适当地址的内核模式设备驱动程序引起的。这个错误检查表明，在提高中断请求级别（IRQL）时，有人试图访问一个无效的地址。其原因是一个坏的内存指针或设备驱动代码的 pageability 问题。

```
*                        Bugcheck Analysis                                    *
*                                                                             *
*******************************************************************************

IRQL_NOT_LESS_OR_EQUAL (a)
An attempt was made to access a pageable (or completely invalid) address at an
interrupt request level (IRQL) that is too high.  This is usually
caused by drivers using improper addresses.
If a kernel debugger is available get the stack backtrace.
Arguments:
Arg1: 0000000000000000, memory referenced
Arg2: 0000000000000002, IRQL
Arg3: 0000000000000000, bitfield :
      bit 0 : value 0 = read operation, 1 = write operation
      bit 3 : value 0 = not an execute operation, 1 = execute operation (only on chips which support this level of status)
Arg4: fffff8006b4f6343, address which referenced memory

Debugging Details:
```

查看出故障时的指令指针以及 irql 情况。

```
7: kd> ln fffff8006b4f6343
Browse module
Set bu breakpoint

(fffff800`6b4f61d0)   nt!KeSetEvent+0x173   |  (fffff800`6b4f6640)   nt!KiExitDispatcher
7: kd> !irql
Debugger saved IRQL for processor 0x7 -- 2 (DISPATCH_LEVEL)
```

查看 trap frame 情况，显示访问了无效的内存地址。

```
7: kd> .trap 0xfffff380a8cf0270
NOTE: The trap frame does not contain all registers.
Some register values may be zeroed or incorrect.
rax=0000000000000000 rbx=0000000000000000 rcx=ffffd983ded27460
rdx=0000000000000000 rsi=0000000000000000 rdi=0000000000000000
rip=fffff8006b4f6343 rsp=fffff380a8cf0400 rbp=ffff94000ffca180
 r8=0000000000000000  r9=0000000000000065 r10=ffffd983af4c28d0
r11=fffff380a8cf03b8 r12=0000000000000000 r13=0000000000000000
r14=0000000000000000 r15=0000000000000000
iopl=0         nv up ei pl nz ac pe cy
nt!KeSetEvent+0x173:
fffff800`6b4f6343 4d8b6d00        mov     r13,qword ptr [r13] ds:00000000`00000000=????????????????
```

查看出问题时的 call stack 情况，显示 kgpm_64.sys 驱动 FAULTING_IP。

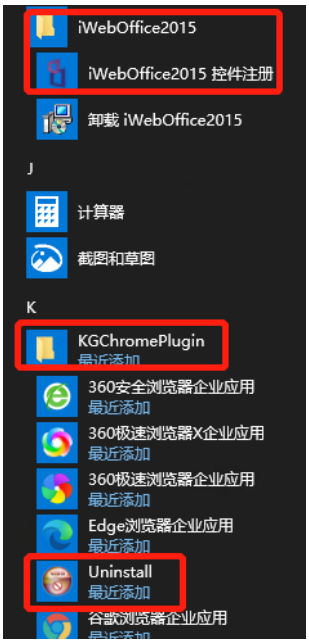
（kgpm_64 调用 KeSetEvent 后 IRQL 提升至 DISPATCH_LEVEL，以至后续的操作出错：Bug Check 0xa: IRQL_NOT_LESS_OR_EQUAL。）

```
7: kd> knL
 # Child-SP          RetAddr           Call Site
00 fffff380`a8cf0128 fffff800`6b66a0e9 nt!KeBugCheckEx
01 fffff380`a8cf0130 fffff800`6b6664d4 nt!KiBugCheckDispatch+0x69
02 fffff380`a8cf0270 fffff800`6b4f6343 nt!KiPageFault+0x454
03 fffff380`a8cf0400 fffff800`82791f03 nt!KeSetEvent+0x173
04 fffff380`a8cf0490 fffff800`6b5b4af5 kgpm_64+0x1f03
05 fffff380`a8cf0550 fffff800`6b65fd5c nt!PspSystemThreadStartup+0x55
06 fffff380`a8cf05a0 00000000`00000000 nt!KiStartSystemThread+0x1c
```

查看 kgpm_64 文件情况。

```
7: kd> lmvm kgpm_64
Browse full module list
start             end                 module name
fffff800`82790000 fffff800`827ad000   kgpm_64    (no symbols)
    Loaded symbol image file: kgpm_64.sys
    Image path: \??\C:\Program Files (x86)\KGChromePlugin\x64\kgpm_64.sys
    Image name: kgpm_64.sys
    Browse all global symbols  functions  data
    Timestamp:        Tue May 26 17:24:43 2020 (5ECCE05B)
    CheckSum:         00018391
    ImageSize:        0001D000
    Translations:     0000.04b0 0000.04e4 0409.04b0 0409.04e4
    Information from resource tables:
```

该文件位置为：C:\Program Files (x86)\KGChromPlugin\x64\kgpm_64.sys。为 2020 年 5 月版本。查询它是**金格 iweboffice 的插件，**请三方应用厂商排查是否存在更新，如无使用必要，可进行卸载后再次观察，问题是否解决。



危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

神州网信
CMIT

发件人: Wei Liang <weiliang@cmgos.com>
发送时间: 2023 年 6 月 26 日 16:14
收件人: Liu Jian <liujian@cmgos.com>
抄送: Wei Liang <weiliang@cmgos.com>
主题: [案例号：CAS-09233-C4V1M3]％ TAM-中再保险用户反馈蓝屏问题 ％初次响应 CMIT:0001812

刘健 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 危亮 。 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-09233-C4V1M3 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
