Hi，毓杰：

如上午电话沟通，目前收集的 dump 分析已完成，正在交由 GSC 团队进行 netmgr 的问题分析，暂无后续支持需要，经您的同意，此 case 将暂做归档处理，以下为案例总结：

Case No： CAS-04678-Z1F4K9

问题描述：

==========

用户反馈目前有三位用户在正常操作中发生电脑蓝屏，并在重启过程中反复蓝屏无法进入系统。

问题总结：

==========

经 dump 分析，造成此次蓝屏的原因为问题发生在调用网络管理驱动 netmgr.sys 后触发 pagefault，在当前 IRQL 较高的情况下(DISPATCH_LEVEL=2)去访问了一个无效的内存地址。需要 GSC 厂商进行排查处理。目前三方厂商正在进一步排查问题原因，暂无后续支持需要

以上，经您的确认，此 case 暂做归档处理，如您后续有其他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

神州网信
CMIT

发件人: Li Qi
发送时间: 2021 年 8 月 25 日 17:53
收件人: '吴毓杰' <win10sup@sdc.icbc.com.cn>

抄送: ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: [案例号: CAS-04678-Z1F4K9] % |P3|ICBC|Windows 10 神州网信政府版电脑蓝屏 % 初次响应 CMIT:0001931

Hi，毓杰:

更新一下目前收到的两个dump 的分析结果。bugcheck一致，均为0xd1。表明在dispatch level 下，netmgr 尝试访问可分页的（或损坏的）内存导致蓝屏。

```
DRIVER_IRQL_NOT_LESS_OR_EQUAL (d1)
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 kernel debugger is available get stack backtrace.
Arguments:
Arg1: ffffd30bf38a7001, memory referenced
Arg2: 0000000000000002, IRQL
Arg3: 0000000000000000, value 0 = read operation, 1 = write operation
Arg4: fffff801898c4b97, address which referenced memory

kd>!irql
Debugger saved IRQL for processor 0x0 -- 2 (DISPATCH_LEVEL)
```

查看 dump 的 callstack 信息，在加载系统驱动时，由 netmgr 引发的 pagefault 是此次蓝屏原因。具体可参见部分 dump 信息:

00 ffffe401`ccb37268 fffff801`7e2725e9 nt!KeBugCheckEx
01 ffffe401`ccb37270 fffff801`7e26e9d4 nt!KiBugCheckDispatch+0x69
02 ffffe401`ccb373b0 fffff801`898c4b97 nt!KiPageFault+0x454
03 ffffe401`ccb37540 fffff801`898c5fce netmgr+0x4b97
04 ffffe401`ccb37590 fffff801`898c96f9 netmgr+0x5fce
05 ffffe401`ccb37650 fffff801`898c99ba netmgr+0x96f9
06 ffffe401`ccb376a0 fffff801`7e123d79 netmgr+0x99ba
07 ffffe401`ccb376f0 fffff801`7e6c96c1 nt!IofCallDriver+0x59

kd> .frame /r 03
03 ffffe401`ccb37540 fffff801`898c5fce netmgr+0x4b97
rax=ffffd30bf38a6fc0 rbx=0000000000000000 rcx=32a9ef303b7c0000
rdx=0000000000000001 rsi=0000000000000006 rdi=0000000000000030
rip=fffff801898c4b97 rsp=ffffe401ccb37540 rbp=ffffd30bf31f9738
r8=0000000000000008 r9=0000000000000065 r10=00000000000000b7
r11=ffffe401ccb37538 r12=fffff801898c0000 r13=ffffd30beeffe940
r14=0000000000000000 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=00000282
netmgr+0x4b97:
fffff801`898c4b97 0fb64c0711   movzx   ecx,byte ptr [rdi+rax+11h]
ds:002b:ffffd30b`f38a7001=??

kd> dq ffffd30bf38a6fc0
ffffd30b`f38a6fc0  00000004`00000001 19a475f8`5020f101

ffffd30b`f38a6fd0  54209102`00005aa4 00005aa4`19a475f8
ffffd30b`f38a6fe0  19a475f8`7a0b0ffe c0a80a01`00005aa4
ffffd30b`f38a6ff0  000063b7`6ce07440 35353535`35353535
ffffd30b`f38a7000  ????????`???????? ????????`????????
ffffd30b`f38a7010  ????????`???????? ????????`????????
ffffd30b`f38a7020  ????????`???????? ????????`????????
ffffd30b`f38a7030  ????????`???????? ????????`????????

进而查看 netmgr 的驱动文件加载情况，可以看到 GSC 的加载信息。

```
0: kd> !mex.mods netmgr -v
Number of modules: loaded: 462 unloaded: 14
Num   Base              End               Module name       Size kb   Checksum   Time stamp           CLR   Arch   Version   Bin Version   Product Name
138 |        71f00000         71f1d000  netmgr_71f00000 |      116 | 000259fa | 2021-06-15 11:43:00 |  No | i386 | 6.0.0.0 | 6.0.0.0     | GSC Desktop terminal security management platform
299 | fffff801898c0000 fffff80189ab8000 | netmgr          |    2,016 | 0003c983 | 2021-06-16 17:49:19 |  No | ???  | 0.0.0.0 | 0.0.0.0     |
```

kd> lmva 0x00000000071f00000
Browse full module list
start end module name
00000000`71f00000  00000000`71f1d000 netmgr_71f00000 (export symbols) netmgr.dll
  Loaded symbol image file: netmgr.dll
  Image path: C:\Windows\System32\Pclient\app\lib\netmgr.dll
  Image name: netmgr.dll
  Browse all global symbols functions data
  Timestamp: Tue Jun 15 19:43:00 2021 (60C89244)
  CheckSum: 000259FA
  ImageSize: 0001D000
  File version: 6.0.0.0
  Product version: 6.0.0.0
  File flags: 0 (Mask 3F)
  File OS: 4 Unknown Win32
  File type: 1.0 App
  File date: 00000000.00000000
  Translations: 0804.04b0
  Information from resource tables:
    ProductName: GSC Desktop terminal security management platform
    ProductVersion: 6.0.0.0
    FileVersion: 6.0.0.0
    FileDescription: GSC FILE
    LegalCopyright: (C)GeneralSoft Corporation. All rights reserved.

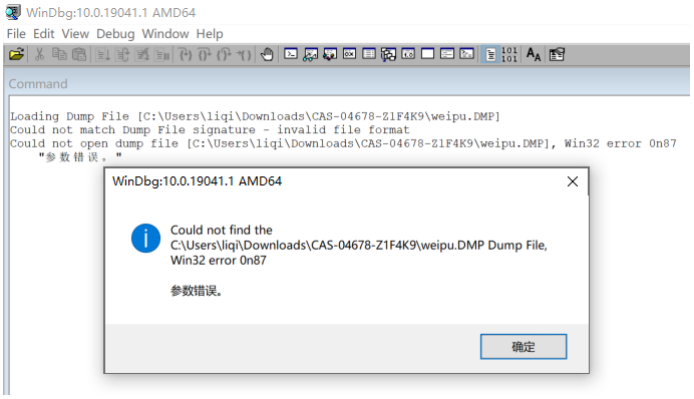
根据用户测试结果，将 TMS 进行降级后，该问题不再复现。与当前 dump 结果表现一致。请联系 GSC，对 C:\Windows\System32\Pclient\app\lib\netmgr.dll 做进一步排查，谢谢。

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

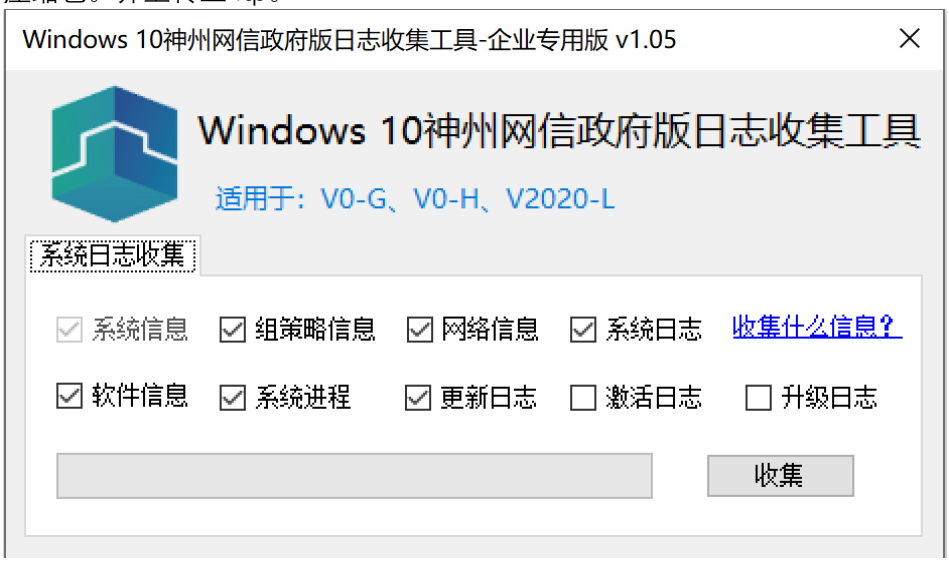
发件人: Li Qi
发送时间: 2021 年 8 月 25 日 11:11
收件人: '吴毓杰' <win10sup@sdc.icbc.com.cn>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: [案例号: CAS-04678-Z1F4K9] % |P3|ICBC|Windows 10 神州网信政府版电脑蓝屏 % 初次响应 CMIT:0001931

Hi，毓杰:

如刚才电话沟通，收取的 dump 文件损坏，无法打开，需要在用户再次发生蓝屏第一次的时候重新收集，并请使用附件工具，收集系统日志并上传至 ftp，谢谢。



使用附件中的 CMGELogCollector.zip 解压后运行，勾选所有项，点击收集，会在桌面生成日志压缩包。并上传至 ftp。



==========

在向 CMIT 提供日志和数据前，请阅读并接受邮件下方隐私声明。

隐私声明

为向您提供本产品的相关技术支持及相关服务，您需要在同意本声明的前提下向神州网信提供为解决系统故障必要的数据和信息，包括但不限于与您相关的个人数据和隐私信息。通常情况下，我们仅需要如下数据以使我们的服务能够更好地满足您的需求：内存转储文件、注册表信息、组策略信息、事件日志、安装应用列表、驱动信息、网络日志或系统补丁等。

神州网信承诺将采取商业上可行及必要措施保护用户提供给神州网信的数据和信息，且仅在解决问题过程中使用。

神州网信保证不对外公开或向第三方提供、公开或共享您提供的数据和信息。

在以下情况下，神州网信对您的数据和信息的披露将不视为违约，具体包括:

(1) 神州网信已获得您的明确授权;

(2) 根据适用法律的要求，神州网信负有披露义务的;

(3) 司法机关或行政机关基于法定程序要求神州网信提供的;

(4) 为维护社会公共利益及神州网信合法权益，在合理范围内进行披露的。

(5) 为了解决您的系统故障问题，神州网信可能会与神州网信的分包商披露您提供的数据和信息。在此情况下，第三方会承担与神州网信同等的隐私保护责任的，神州网信会在合理范围内对您的信息进行披露。

如果您欲提供的数据和信息中包含对您重要的保密信息以及商业秘密，在您向神州网信提供上述数据和信息前，务必对上述数据和信息进行脱敏处理，否则请不要提供该信息给神州网信。作为一家商业软件公司，神州网信在商业可行的前提下，已为用户的数据和信息保护做了极大的努力，但是仍然不能保证现有的安全技术措施使您的数据和信息等不受任何形式的损失。您对上述情况充分知情，且不会因此追究神州网信的法律责任。

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 8 月 25 日 10:39
收件人: 吴毓杰 <win10sup@sdc.icbc.com.cn>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: [案例号: CAS-04678-Z1F4K9] % |P3|ICBC|Windows 10 神州网信政府版电脑蓝屏 % 初次响应 CMIT:0001931

Hi，毓杰:

如刚才电话沟通，我谨以此邮件阐述我们双方针对这个问题所涉及范围界定:

问题定义:

用户反馈目前有三位用户在正常操作中发生电脑蓝屏，并在重启过程中反复蓝屏无法进入系统。

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。

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 <liqi@cmgos.com>
发送时间: 2021 年 8 月 25 日 9:52
收件人: 吴毓杰 <win10sup@sdc.icbc.com.cn>

抄送: Li Qi <liqi@cmgos.com>
主题: [案例号: CAS-04678-Z1F4K9] % |P3|ICBC|Windows 10 神州网信政府版电脑蓝屏 % 初次响应 CMIT:0001931

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-04678-Z1F4K9 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
