

胡先生，您好！

很高兴与您电话沟通，根据沟通的结果，我将暂时归档此问题。**案例归档后您会收到调查问卷的邮件，希望可以对我们的服务进行评价。**

工单的归档并不会影响我们为您提供技术支持服务，如果您的问题复现，或有新的问题出现，您也可以致电我们的技术支持热线 4008180055。

案例总结

案例范围：用户安装一些财务软件后不定时发生蓝屏现象，
KERNEL_SECURITY_CHECK_FAILURE (139)

案例进展：由于查看 ntfs.sys 出现再 bad memory 里，建议进行 Windows 更新。但更新过程出现问题，定位与镜像定制有关系，等待重新安装系统后再次复现问题。且由于蓝屏时可能有其他 Module 写坏内存导致，建议开启 special pool 再次触发蓝屏收集 dump。

由于涉及到驱动，要再查看 bad memory 是哪个驱动引起的，必须要开启 special pool 了。您可以和用户商量是否要开启，但务必提示用户开启后的风险。

Important:

1. 开启 special pool 可能会引起系统性能下降，导致蓝屏问题更容易触发。

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

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: 2020 年 6 月 3 日 10:37

收件人: 'huzuo chen' <huzuo chen@qq.com>

抄送: CRM Case Email <casemail@cmgos.com>

主题: 回复: [案例号: CAS-02227-X4W1B1] % 西安中御智诚信息技术有限公司帮陕西省煤田地质集团有限公司反馈电脑蓝屏问题 % 初次响应 CMIT:0001409

胡先生, 您好

收到, 您可以使用纯净版镜像安装后测试 Windows 更新, 再观察蓝屏现象是否还会复现, 如果有问题请回复此邮件,

贾伟 Jia Wei

神州网信技术有限公司

服务电话: 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: huzuo chen <huzuo chen@qq.com>

发送时间: 2020 年 6 月 1 日 17:54

收件人: Jia Wei <jiawei@cmgos.com>

抄送: CRM Case Email <casemail@cmgos.com>

主题: 回复: 回复: 回复: [案例号: CAS-02227-X4W1B1] % 西安中御智诚信息技术有限公司帮陕西省煤田地质集团有限公司反馈电脑蓝屏问题 % 初次响应 CMIT:0001409

镜像问题, 我先解决下镜像问题。

---原始邮件---

发件人: "Jia Wei" <jiawei@cmgos.com>

发送时间: 2020 年 6 月 1 日 (周一) 下午 4:47

收件人: "huzuochen" <huzuochen@qq.com>;

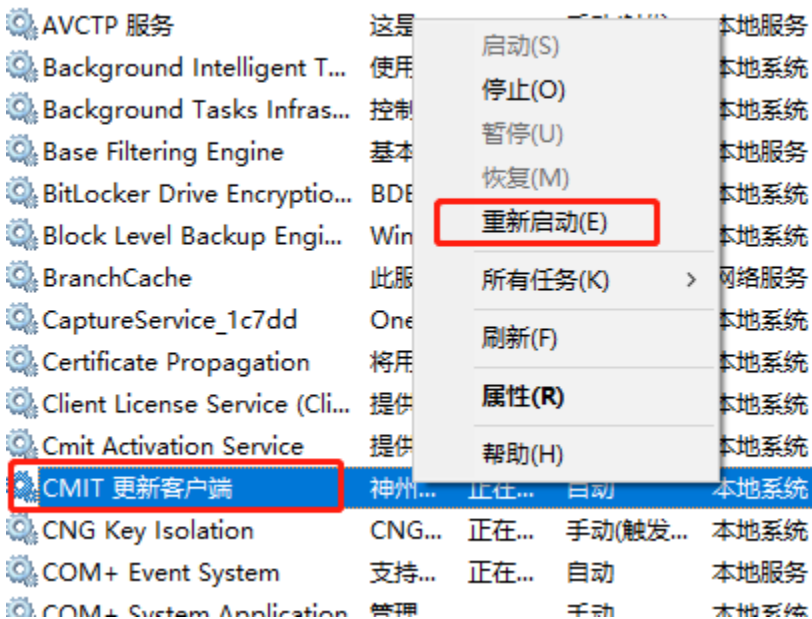
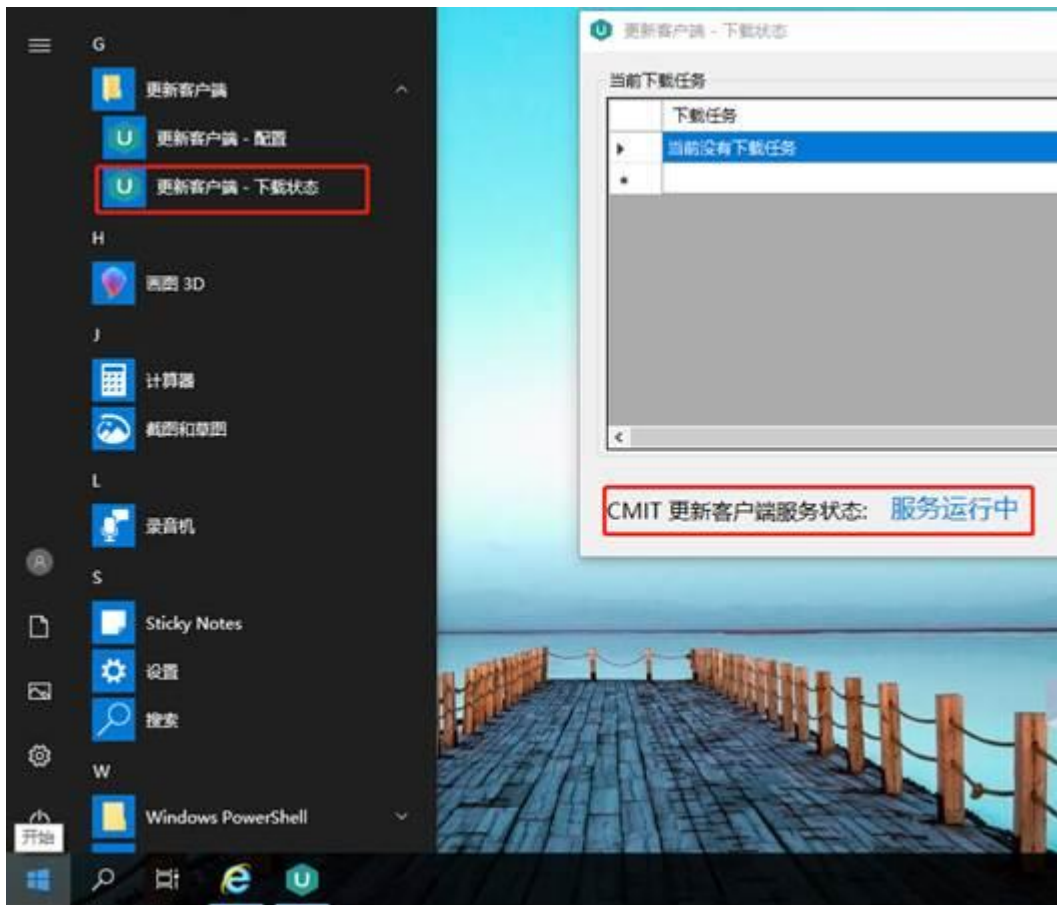
抄送: "CRM Case Email" <casemail@cmgos.com>;

主题: 回复: 回复: [案例号: CAS-02227-X4W1B1] % 西安中御智诚信息技术有限公司帮陕西省煤田地质集团有限公司反馈电脑蓝屏问题 % 初次响应 CMIT:0001409

胡先生, 您好

我这边又查找了相关文档, 如果尝试仍失败, 只能收集数据进行分析

1. 查看更新客户端状态, 如果状态不对, 可以重启此服务。



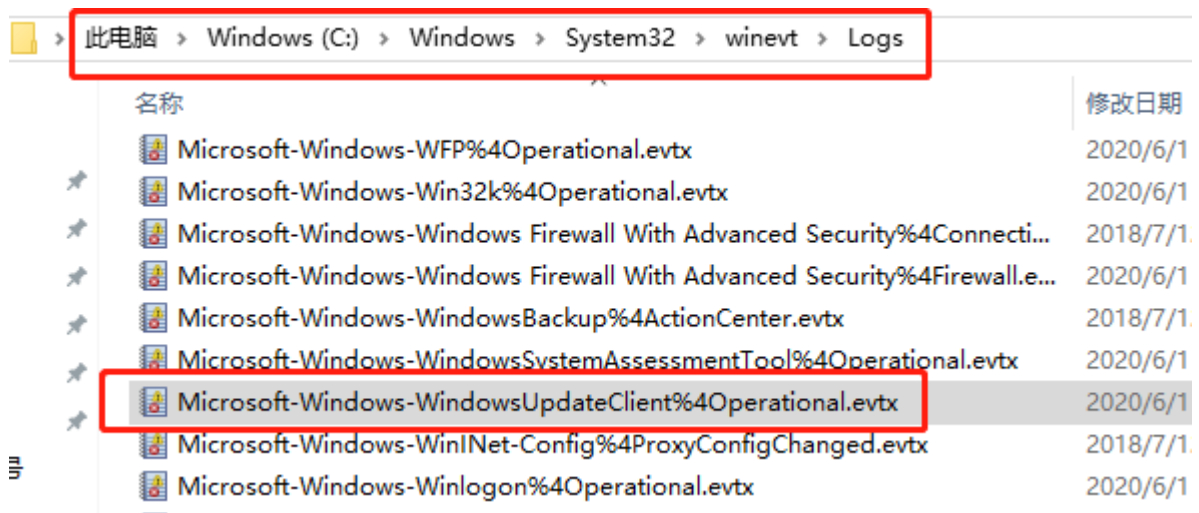
2. 清除当前的 BITS 队列；

以管理员身份运行 CMD，输入：bitsadmin.exe /reset /allusers，再手动点击 Windows 更新进行下载

3. 收集 CBS Log、Windowsupdate.Log、Windows 更新事件日志

日志路径:

- 1 C:\Windows\Logs\CBS;
- 1 以管理员运行 Powershell, 运行命令: `get-windowsupdate-log`, 在桌面会生成 Windowsupdate 日志,
- 1 C:\Windows\System32\winevt\logs 文件夹, 找到 Microsoft-Windows-WindowsUpdateClient



临时解决方案: 到如下网站手动下载并双击安装补丁包, 首先建议下载 KB4551853 累计更新, 其他为截图对应的其他补丁包

<https://support.cmgos.com/v2020lupdatesummary>

版本V2020-L 更新(操作系统内部版本17763.774)

重要首先下载安装

更新内容/操作系统内部版本号	生效日期	文档编号
17763.1217	2020/5/13	KB4551853
.NET Framework 3.5, 4.7.2 和 4.8 累积更新	2020/5/13	KB4556441
解决双硬盘情况下，进入系统后D盘存在testlogmsg.txt文件的问题	2020/4/24	CKB20200408
提高 Windows 10 神州网信政府版服务堆栈的稳定性	2020/4/15	KB4549947
17763.1158	2020/4/15	KB4549949
提高 Windows 10 神州网信政府版服务堆栈的稳定性	2020/3/11	KB4523204
17763.1098	2020/3/11	KB4538461
提高 Windows 10 神州网信政府版服务堆栈的稳定性	2020/3/11	KB4539571
[已撤回] Windows 10神州网信政府版的安全更新程序	2020/2/12	KB4524244
.NET Framework 3.5, 4.7.2 和 4.8 累积更新	2020/2/12	KB4538122
修复Adobe Flash Player 中的漏洞	2020/2/12	KB4537759
英特尔CPU的微代码更新	2020/2/12	KB4494174
17763.1039	2020/2/12	KB4532691
17763.973	2020/1/15	KB4534273

贾伟 Jia Wei

神州网信技术有限公司

服务电话： 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: huzuochen <huzuochen@qq.com>

发送时间: 2020 年 6 月 1 日 16:00

收件人: Jia Wei <jiawei@cmgos.com>

抄送: CRM Case Email <casemail@cmgos.com>

主题: 回复: [案例号: CAS-02227-X4W1B1] % 西安中御智诚信息技术有限公司
帮陕西省煤田地质集团有限公司反馈电脑蓝屏问题 % 初次响应 CMIT:0001409

你好, 运行命令结果为 True。

第二个方法已试过不行, 刚在网上找的办法。

包括对比了

windows update, 开启

app readiness, 停止

Cryptographic Services, 启动

Background Intelligent Transfer Service, 停止

Windows Installer 停止

---原始邮件---

发件人: "Jia Wei" <jiawei@cmgos.com>

发送时间: 2020 年 6 月 1 日 (周一) 下午 3:32

收件人: " 胡佐臣" <huzuochen@qq.com>;

抄送: "CRM Case Email" <casemail@cmgos.com>;

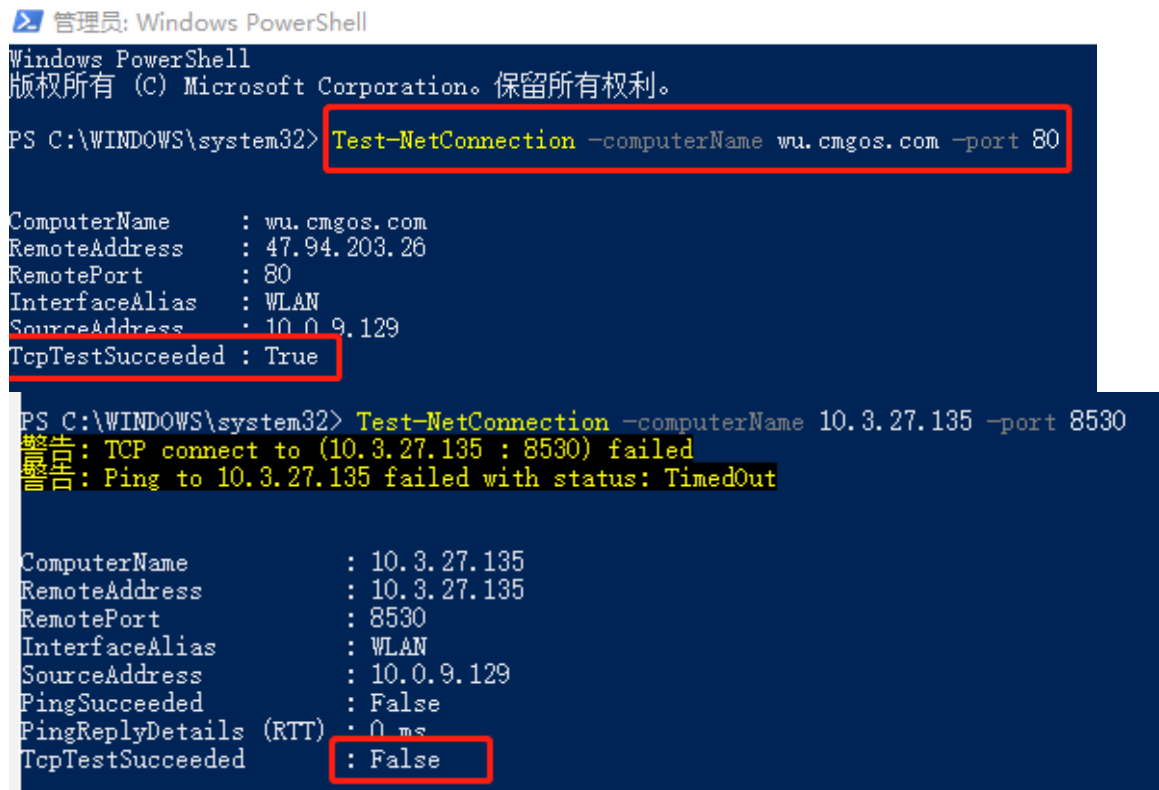
主题: 回复: [案例号: CAS-02227-X4W1B1] % 西安中御智诚信息技术有限公司
帮陕西省煤田地质集团有限公司反馈电脑蓝屏问题 % 初次响应 CMIT:0001409

胡先生, 您好

查看您的截图看起来是网络问题。先检查能否连接到更新服务器:

1. 同时按下“Windows 键+X”, 按下“A”, 选择”是“以管理员身份运行 PowerShell;
2. 运行 `Test-NetConnection -computerName wu.cmgos.com -port 80` (可复制此段内容) 命令, 查看结果 `TcpTestSucceeded` 是否未 `True`;

以下截图分别为“成功”、“失败”示例:



The image contains two screenshots of a Windows PowerShell terminal window running as Administrator. The first screenshot shows a successful connection test to wu.cmgos.com on port 80, with 'TcpTestSucceeded' set to 'True'. The second screenshot shows a failed connection test to 10.3.27.135 on port 8530, with 'TcpTestSucceeded' set to 'False' and warning messages about failed TCP connect and ping.

```
管理员: Windows PowerShell
Windows PowerShell
版权所有 (C) Microsoft Corporation。保留所有权利。

PS C:\WINDOWS\system32> Test-NetConnection -computerName wu.cmgos.com -port 80

ComputerName      : wu.cmgos.com
RemoteAddress     : 47.94.203.26
RemotePort        : 80
InterfaceAlias    : WLAN
SourceAddress     : 10.0.9.129
TcpTestSucceeded  : True




PS C:\WINDOWS\system32> Test-NetConnection -computerName 10.3.27.135 -port 8530
警告: TCP connect to (10.3.27.135 : 8530) failed
警告: Ping to 10.3.27.135 failed with status: TimedOut

ComputerName      : 10.3.27.135
RemoteAddress     : 10.3.27.135
RemotePort        : 8530
InterfaceAlias    : WLAN
SourceAddress     : 10.0.9.129
PingSucceeded     : False
PingReplyDetails (RTT) : 0 ms
TcpTestSucceeded  : False
```


如果网络不行，建议排查网络，本地网络监控软件，或使用其他方式，例如手机热点方式连接网络

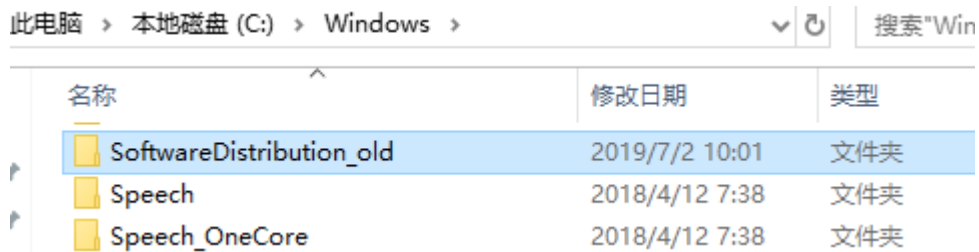
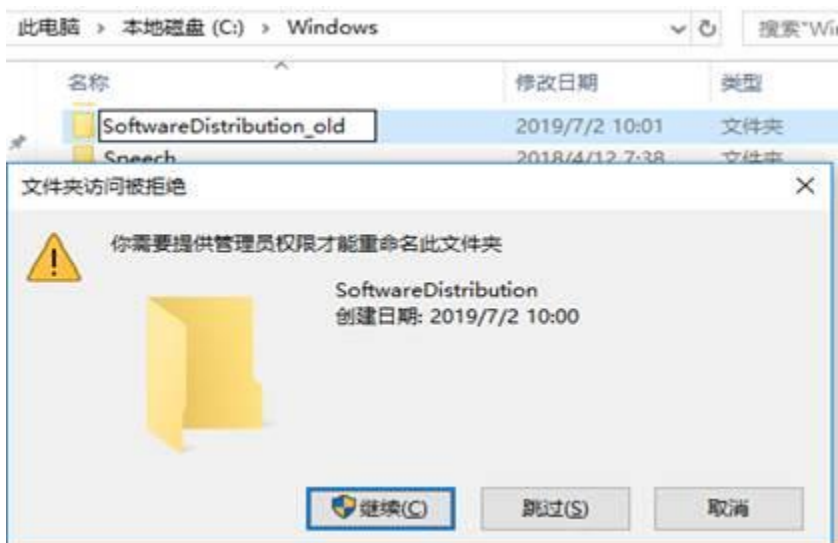
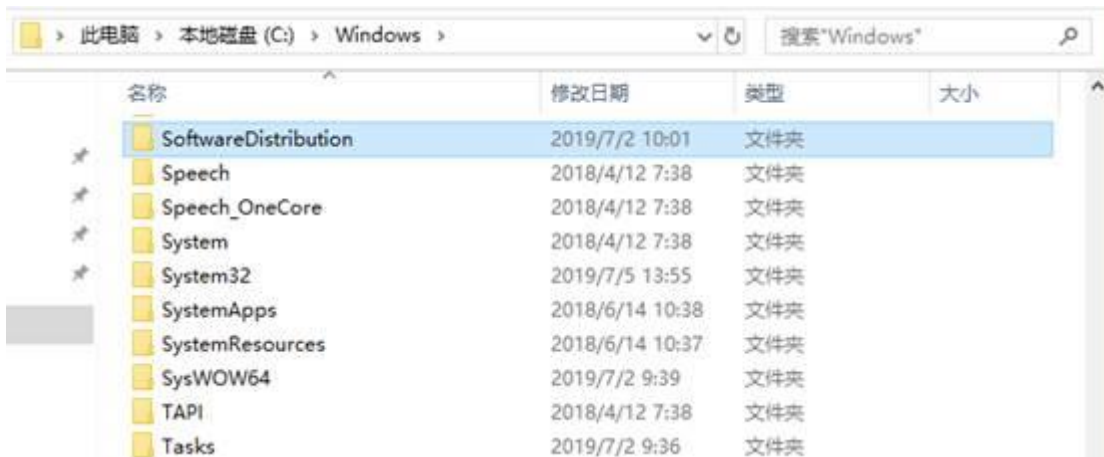
二、重置 SoftwareDistribution 文件夹

1. 键入 Windows 键+R 键，调出运行栏，输入 services.msc，调出服务框，找到并停止 Windows update 服务；

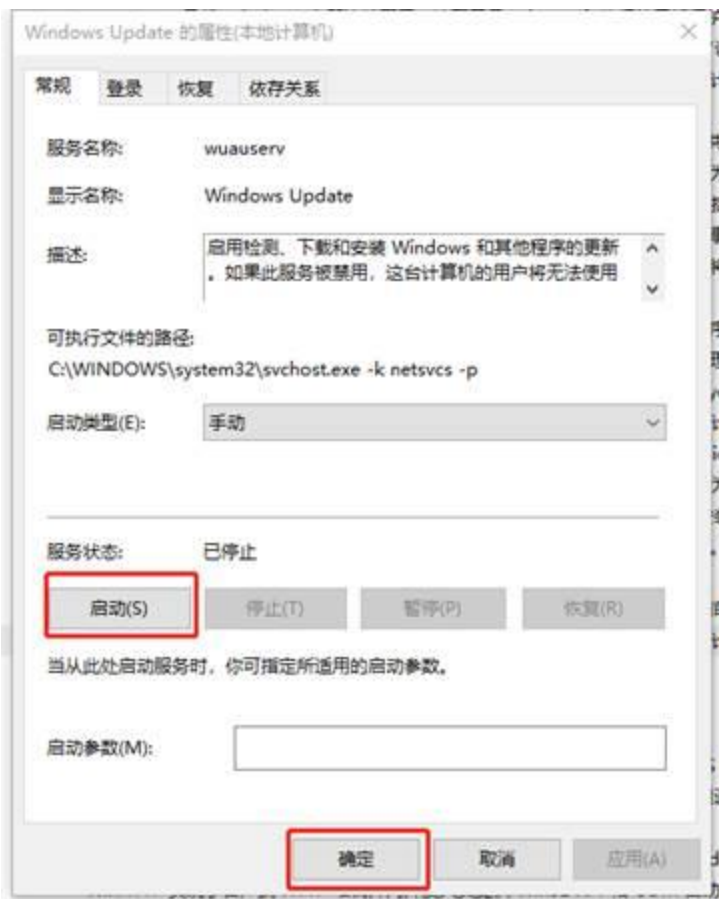
	Windows Time	维护...		手动(触发...	本地服务
	Windows Update	启用...	正在	手动(触发...	本地系统
	Windows Update Medic ...	Ena...	正在	手动	本地系统



2. 导航至 C:\Windows，找到 SoftwareDistribution 文件夹。将此文件夹重命名，如 SoftwareDistribution_old;



3. 同时按下 Windows 键+R 键，调出运行栏，输入 services.msc，调出服务框，找到并启用 Windows update 服务；



4. 再到设置 -> 更新和安全 -> 点击 Windows 更新-重试

Windows 更新

*某些设置由你的组织来管理

[查看配置的更新策略](#)



更新可用

上次检查时间: 今天, 14:00

2019-适用于 Windows 10 Version 1803 的 06 累积更新, 适合基于 x64 的系统 (KB4509478)

状态: 正在下载 - 37%

2019-适用于 Windows 10 Version 1803 的 06 更新, 适用于基于 x64 的系统 (KB4494451)

状态: 正在等待安装

2019-适用于 Adobe Flash Player for Windows 10 Version 1803 的 06 安全更新, 适用于基于 x64 的系统 (KB4503308)

状态: 正在等待安装

2019-适用于 Windows 10 Version 1803 的 05 服务堆栈更新, 适合基于 x64 的系统 (KB4497398)

状态: 正在等待安装

用于基于 x64 的系统的 Windows 10 Version 1803 的 Adobe Flash Player 更新 (KB4462930)

状态: 正在等待安装

2018-适用于 Windows 10 Version 1803 的 09 更新, 适用于基于 x64 的系统 (KB4456655)

状态: 正在等待安装

*我们将自动下载更新, 除非你使用的是按流量计费连接(可能会收费)。在这种情况下, 我们只会自动下载确保 Windows 流畅运行所必需的更新。更新下载后, 我们将要求你进行安装。

1. 请问能否直接复制 ntfs.sys 文件进行替换。

理论上可以复制并替换此文件, 但必须时同一版本的文件。但我们仍建议先升级更新。

2. 开启 special pool , 是还需要继续收集蓝屏日志吗

是的, 开启 special pool 之后, 如果有驱动程序读/写越界会抓取当时的内存信息。

贾伟 Jia Wei

神州网信技术有限公司

服务电话： 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： 胡佐臣 <huzuochen@qq.com>

发送时间：2020 年 6 月 1 日 14:43

收件人：Jia Wei <jiawei@cmgos.com>

抄送：CRM Case Email <casemail@cmgos.com>

主题：回复：回复：回复：[案例号：CAS-02227-X4W1B1] % 西安中御智诚信息技术有限公司帮陕西省煤田地质集团有限公司反馈电脑蓝屏问题 % 初次响应
CMIT:0001409

已收到。

1. 请问能否直接复制 ntfs.sys 文件进行替换。
2. 开启 special pool ，是还需要继续收集蓝屏日志吗

原始邮件

发件人：“Jia Wei”< jiawei@cmgos.com >;

发件时间：2020/6/1 2:03 (UTC+00:00 伦敦、都柏林、里斯本时间)

收件人：“ 胡佐臣”< huzuochen@qq.com >;

抄送人：“CRM Case Email”< casemail@cmgos.com >;

主题：回复：回复：[案例号：CAS-02227-X4W1B1] % 西安中御智诚信息技术有限公司帮陕西省煤田地质集团有限公司反馈电脑蓝屏问题 % 初次响应 CMIT:0001409

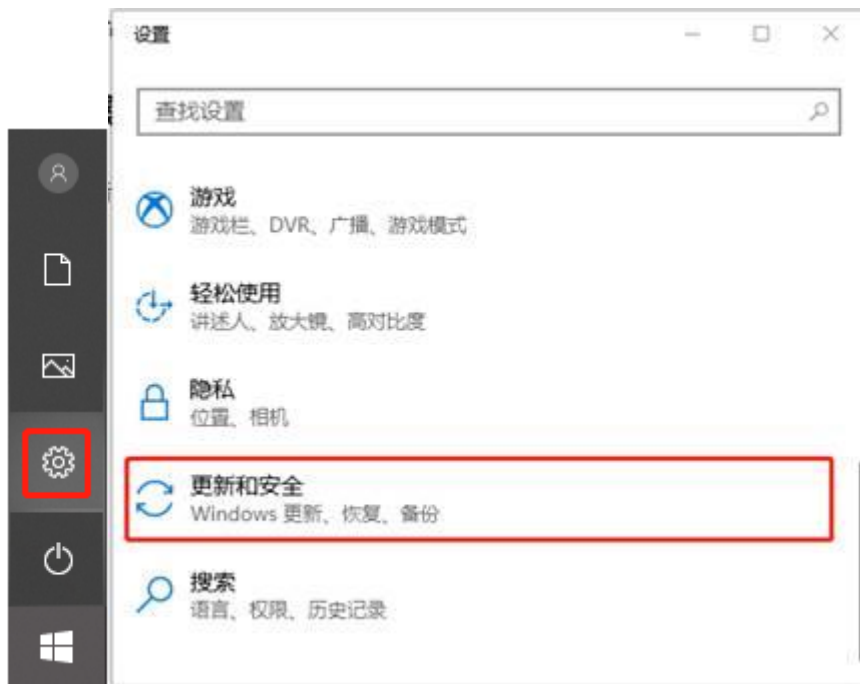
胡先生，您好

根据您所反馈的 dump 文件，查看对应引用 bad memory 的地址，发现对应的是 Ntfs.sys 驱动程序。

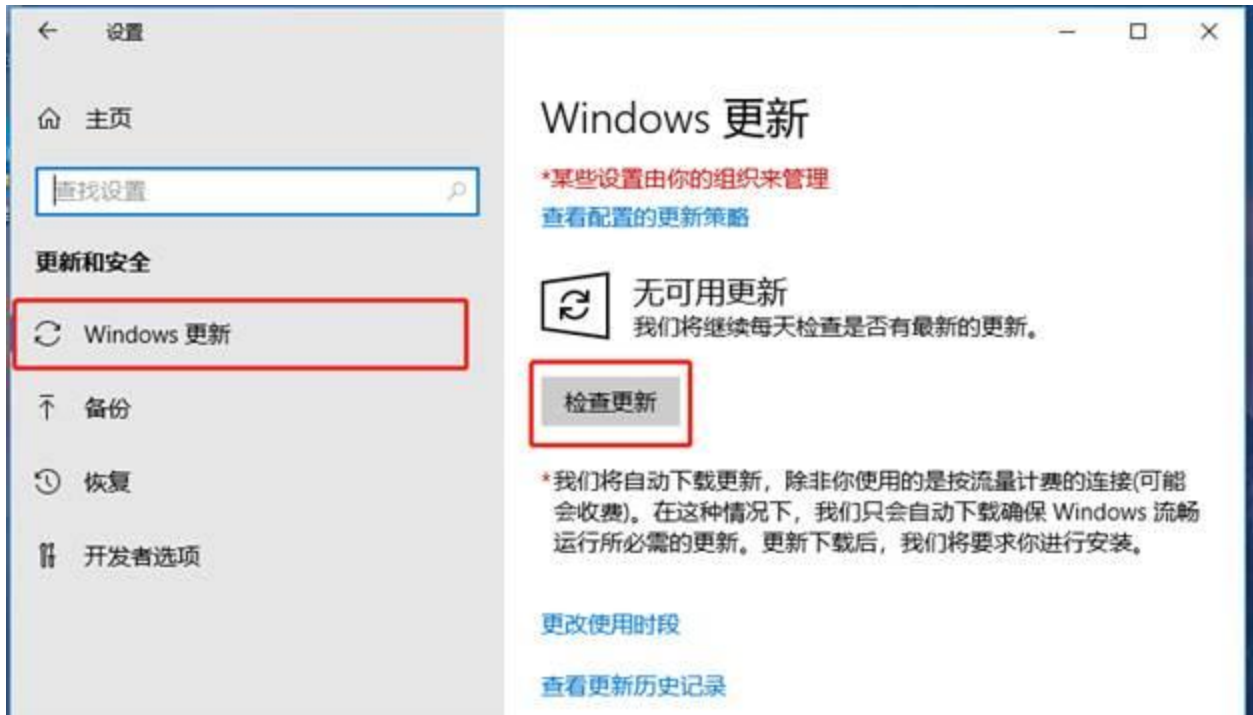
此驱动为系统出厂自带驱动，建议操作如下：

进行系统更新，将 ntfs.sys 升级至 10.0.17763.1098

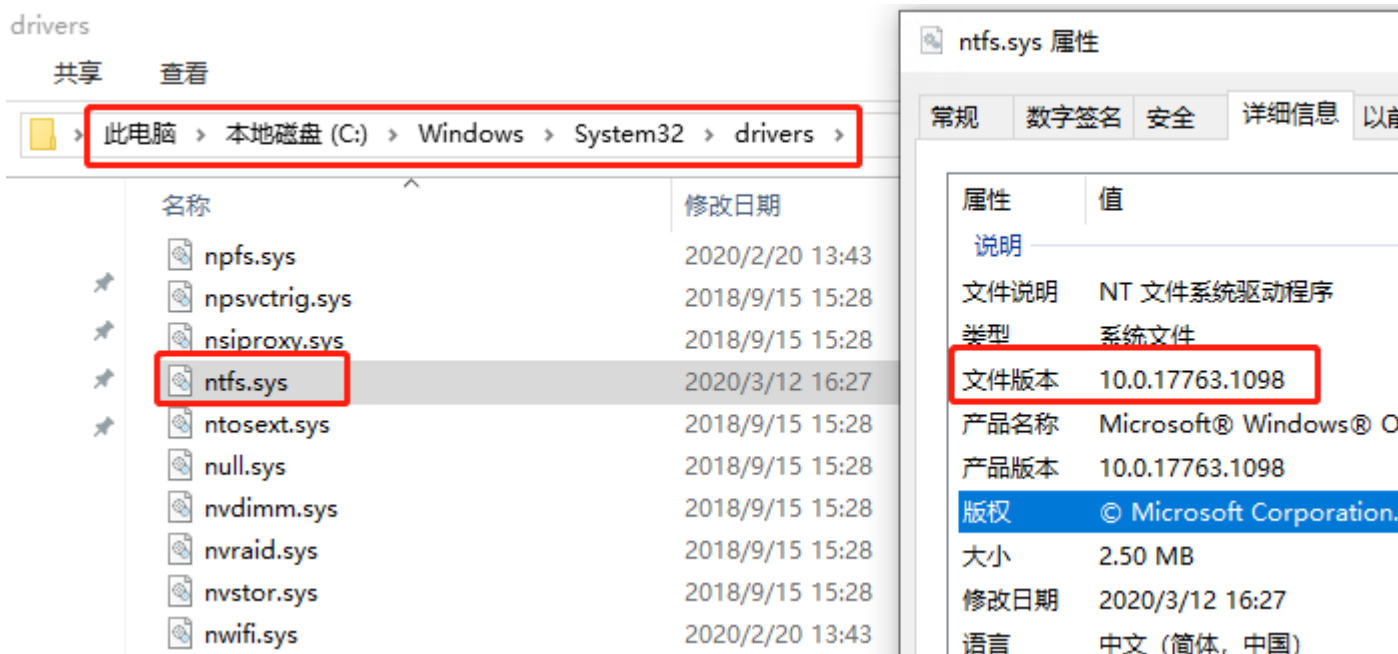
1. 点击“开始”按钮 -> 设置。打开设置界面
2. 面，选择“更新和安全”。



2. 在“Windows 更新”页面，选择“检查更新”，查看是否存在可供更新的版本。



3. 重启后在如下路径查看 ntfs.sys 属性，确认详细信息是否升级至对应版本。



由于涉及到驱动，要再查看 bad memory 是哪个驱动引起的，必须要开启 special pool 了。您可以和用户商量是否要开启，但务必提示用户开启后的风险。

Important:

1. 开启 special pool 可能会引起系统性能下降，导致蓝屏问题更容易触发。

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

2. 关闭 special pool

Dump 分析:

```
3: kd> !addressffff807376ef014
```

```
Mapping user range ...
```

```
Mapping system range ...
```

```
Mapping non addressable range ...
```

```
Mapping page tables...
```

```
Mapping hyperspace...
```

```
Mapping HAL reserved range...
```

```
Mapping User Probe Area...
```

```
Mapping system shared page...
```

```
Mapping system cache working set...
```

```
Mapping loader mappings...
```

```
Mapping system PTEs...
```

```
Mapping system paged pool...
```

```
Mapping session space...
```

```
Mapping dynamic system space...
```

```
Mapping PFN database...
```

```
Mapping non paged pool...
```

```
Mapping VAD regions...
```

```
Mapping module regions...
```

```
Mapping process, thread, and stack regions...
```

```
Mapping system cache regions...
```

Usage:	Module
Base Address:	fffff807`375f0000
End Address:	fffff807`3787d000
Region Size:	00000000`0028d000
VA Type:	BootLoaded
Module name:	Ntfs.sys

```
Module
```

```
path: [\SystemRoot\System32\Drivers\Ntfs.sys]
```

```
3: kd> lmDvm ntfs*
```

Browse full module list

```
start                                end                                module
name
fffff807`375f0000 fffff807`3787d000  Ntfs          # (no
symbols)
```

Loaded symbol image file: Ntfs.sys

Mapped memory image file:

C:\ProgramData\Dbg\sym\Ntfs.sys\3885B4CF28d000\Ntfs.sys

Image path: \SystemRoot\System32\Drivers\Ntfs.sys

Image name: Ntfs.sys

Browse all global symbols functions data

Image was built with /Brepro flag.

Timestamp: 3885B4CF (This is a reproducible build
file hash, not a timestamp)

Checksum: 0028A9FA

ImageSize: 0028D000

File version: 10.0.17763.592

Product version: 10.0.17763.592

File flags: 0 (Mask 3F)

File OS: 40004 NT Win32

File type: 3.7 Driver

File date: 00000000.00000000

Translations: 0409.04b0

Information from resource tables:

CompanyName: Microsoft Corporation

ProductName: Microsoft® Windows® Operating

System

InternalName: ntfs.sys

OriginalFilename: ntfs.sys

ProductVersion: 10.0.17763.592

FileVersion: 10.0.17763.592 (WinBuild.160101.0800

)

FileDescription: NT File System Driver

LegalCopyright: © Microsoft Corporation. All rights

reserved.

贾伟 Jia Wei

神州网信技术有限公司

服务电话： 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： 2020 年 5 月 29 日 14:50

收件人： ' 胡佐臣' <huzuochen@qq.com>

抄送： CRM Case Email <casemail@cmgos.com>

主题： 回复： [案例号： CAS-02227-X4W1B1] % 西安中御智诚信息技术有限公司
帮陕西省煤田地质集团有限公司反馈电脑蓝屏问题 %初次响应 CMIT:0001409

胡先生，您好

收到您的 dump 文件，我将立刻进行下载分析

贾伟 Jia Wei

神州网信技术有限公司

服务电话： 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： 胡佐臣 <huzuochen@qq.com>

发送时间： 2020 年 5 月 28 日 17:50

收件人： Jia Wei <jiawei@cmgos.com>

抄送： CRM Case Email <casemail@cmgos.com>

主题： 回复： 回复： 回复： [案例号： CAS-02227-X4W1B1] % 西安中御智诚信息技
术有限公司帮陕西省煤田地质集团有限公司反馈电脑蓝屏问题 %初次响应
CMIT:0001409

你好。 5 月 28 日新产生的蓝屏日志已经上传到 FTP，请查看。

原始邮件

发件人: "Jia Wei"<jiawei@cmgos.com>;

发件时间: 2020/5/27 5:55 (UTC+00:00 伦敦、都柏林、里斯本时间)

收件人: "胡佐臣"<huzuochen@qq.com>;

抄送人: "CRM Case Email"<casemail@cmgos.com>;

主题: 回复:回复: [案例号: CAS-02227-X4W1B1] % 西安中御智诚信息技术有限公司帮陕西省煤田地质集团有限公司反馈电脑蓝屏问题 %初次响应 CMIT:0001409

胡先生, 您好

根据我们之前的电话沟通结果, 如果有新的蓝屏 Full Dump 产生, 可以随时压缩后上传 sftp 服务器。我将继续观察此案例 1 周时间。

贾伟 Jia Wei

神州网信技术有限公司

服务电话: 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: 2020 年 5 月 19 日 10:20

收件人: '胡佐臣' <huzuochen@qq.com>

抄送: CRM Case Email <casemail@cmgos.com>

主题: 回复: [案例号: CAS-02227-X4W1B1] % 西安中御智诚信息技术有限公司帮陕西省煤田地质集团有限公司反馈电脑蓝屏问题 %初次响应 CMIT:0001409

胡先生，您好

非常感谢反馈，如果有新的蓝屏 Full Dump 产生，可以随时压缩后上传 sftp 服务器。

上传后请回复此邮件，我将安排第一时间下载。谢谢

贾伟 Jia Wei

神州网信技术有限公司

服务电话： 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： 胡佐臣 <huzuochen@qq.com>

发送时间：2020 年 5 月 19 日 10:05

收件人：Jia Wei <jiawei@cmgos.com>

抄送：CRM Case Email <casemail@cmgos.com>

主题：回复：回复：[案例号：CAS-02227-X4W1B1] % 西安中御智诚信息技术有限公司帮陕西省煤田地质集团有限公司反馈电脑蓝屏问题 %初次响应

CMIT:0001409

已将采集的 appwiz.cpl 信息上传 FTP，客户那边提供的是拍照，非截图，不好意思，辛苦了。

日志方面目前没有进展，之前说的采集工具因涉及隐私客户不同意使用。

原始邮件

发件人：“Jia Wei”<jiawei@cmgos.com>;

发件时间：2020/5/19 1:40 (UTC+8:00 伦敦、都柏林、里斯本时间)

收件人：“ 胡佐臣”<huzuochen@qq.com>;

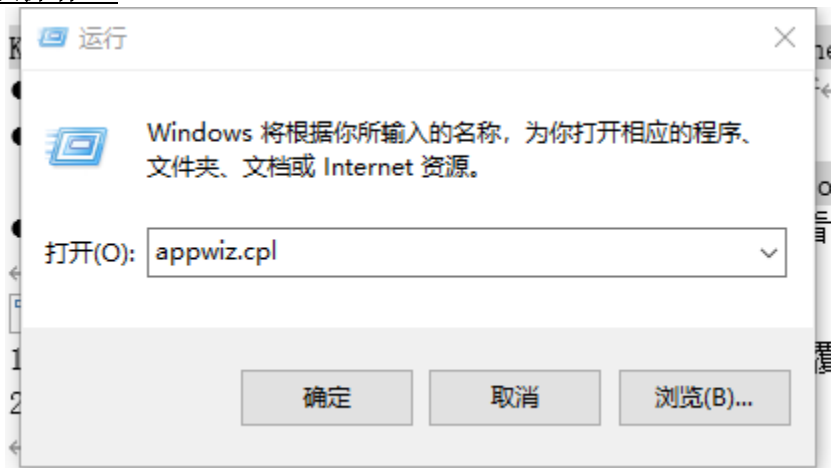
抄送人：“CRM Case Email”<casemail@cmgos.com>;

主题：回复：[案例号：CAS-02227-X4W1B1] % 西安中御智诚信息技术有限公司帮陕西省煤田地质集团有限公司反馈电脑蓝屏问题 %初次响应 CMIT:0001409

胡先生，您好

如果此案例数据收集有进展，您可以回复此邮件，谢谢。

建议操作：



组织 ▾		
名称	发布者	安装时间
Google Chrome	Google LLC	2020/5/8
Adobe Flash Player 32 PPAPI	Adobe	2020/4/24
FusionCompute-ClientIntegrationPlugin	Huawei Technologies Co., Ltd	2020/4/23
SSH Secure Shell		2020/4/23

数据上传

Filezilla client 端下载 URL: <https://filezilla-project.org/download.php?type=client>

主机: sftp://ocean.cmgos.com

用户名为: sxmtdzjt

端口: 22222

密码: GwvQ7Z32

贾伟 Jia Wei

神州网信技术有限公司

服务电话: 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: 2020 年 5 月 15 日 15:03

收件人: 'huzuochen' <huzuochen@qq.com>

抄送: CRM Case Email <casemail@cmgos.com>

主题: 回复: [案例号: CAS-02227-X4W1B1] % 西安中御智诚信息技术有限公司
帮陕西省煤田地质集团有限公司反馈电脑蓝屏问题 %初次响应 CMIT:0001409

胡先生, 您好!

收到您的邮件, 如果有反馈可回复此邮件。

贾伟 Jia Wei

神州网信技术有限公司

服务电话: 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: huzuochen <huzuochen@qq.com>

发送时间: 2020 年 5 月 12 日 14:53

收件人: Jia Wei <jiawei@cmgos.com>

抄送: CRM Case Email <casemail@cmgos.com>

主题: 回复: 回复: 回复: [案例号: CAS-02227-X4W1B1] % 西安中御智诚信息技
术有限公司帮陕西省煤田地质集团有限公司反馈电脑蓝屏问题 %初次响应
CMIT:0001409

好的, 还没有去客户那里。

——原始邮件——

发件人: "Jia Wei" <jiawei@cmgos.com>

发送时间: 2020 年 5 月 12 日 (周二) 下午 2:44

收件人: " 胡佐臣" <huzuochen@qq.com>;

抄送: "CRM Case Email" <casemail@cmgos.com>;

主题: 回复: 回复: [案例号: CAS-02227-X4W1B1] % 西安中御智诚信息技
术有限公司帮陕西省煤田地质集团有限公司反馈电脑蓝屏问题 %初次响应 CMIT:0001409

胡先生，您好！

您可以按照上封邮件“建议操作”的步骤进行数据收集，如果完成可回复此邮件通知我即可。

贾伟 Jia Wei

神州网信技术有限公司

服务电话： 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](mailto:jiawei@cmgos.com) | visit: www.cmgos.com

发件人： Jia Wei

发送时间： 2020 年 5 月 9 日 11:36

收件人： ' 胡佐臣' <huzuochen@qq.com>

抄送： CRM Case Email <casemail@cmgos.com>

主题： 回复： [案例号： CAS-02227-X4W1B1] % 西安中御智诚信息技术有限公司
帮陕西省煤田地质集团有限公司反馈电脑蓝屏问题 %初次响应 CMIT:0001409

胡先生，您好！

案例进展：

KERNEL_SECURITY_CHECK_FAILURE (139) A kernel component has corrupted a critical data structure.

1 由于不是 full dump 文件，所以暂时无法进行深入分析

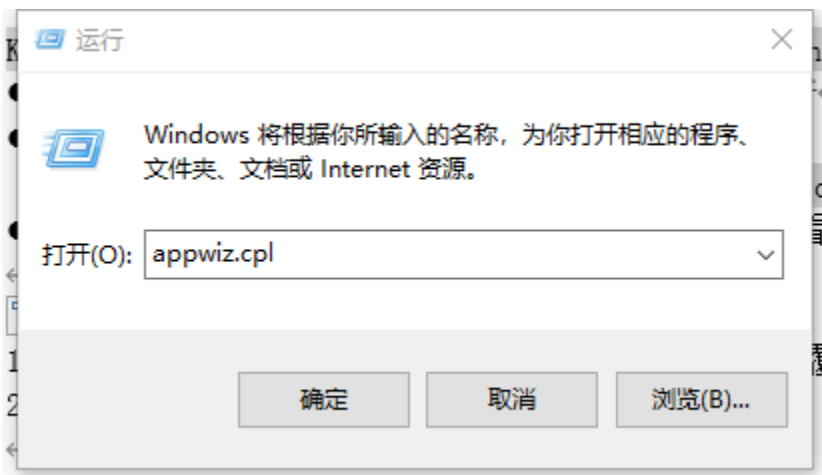
1 报错参数显示

```
Arg1: 00000000000000003, A LIST_ENTRY has been corrupted (i.e. double remove).
```

1 数据链表崩溃，根据之前同样报错信息的案例信息来看，此报错大概率与三方软件的驱动有关系，比如.sys 文件。

建议操作：

1. 继续收集 full dump 文件。由于新生成的 dump 文件会覆盖掉之前的，所以如果出现蓝屏现象，压缩并上传最新的 full dump 文件



1. 将安装的软件列表截图例如下面所示，务必截全名称和版本信息

组织 ▼		
名称	发布者	安装时间
Google Chrome	Google LLC	2020/5/8
Adobe Flash Player 32 PPAPI	Adobe	2020/4/24
FusionCompute-ClientIntegrationPlugin	Huawei Technologies Co., Ltd	2020/4/23
SSH Secure Shell		2020/4/23

数据上传

Filezilla client 端下载 URL: <https://filezilla-project.org/download.php?type=client>

主机: sftp://ocean.cmgos.com

用户名为: sxmtdzjt

端口: 22222

密码: GwvQ7Z32

贾伟 Jia Wei
神州网信技术有限公司
服务电话： 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: 2020 年 5 月 7 日 16:42
收件人: ' 胡佐臣' <huzuochen@qq.com>
抄送: CRM Case Email <casemail@cmgos.com>
主题: 回复:回复:回复: [案例号: CAS-02227-X4W1B1] % 西安中御智诚信息技术有限公司帮陕西省煤田地质集团有限公司反馈电脑蓝屏问题 %初次响应
CMIT:0001409

好的，下载 dump 文件之后我们马上开始案例升级流程。

贾伟 Jia Wei
神州网信技术有限公司
服务电话： 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: 2020 年 5 月 7 日 12:56
收件人: ' 胡佐臣' <huzuochen@qq.com>
抄送: CRM Case Email <casemail@cmgos.com>
主题: 回复:回复:回复: [案例号: CAS-02227-X4W1B1] % 西安中御智诚信息技术有限公司帮陕西省煤田地质集团有限公司反馈电脑蓝屏问题 %初次响应
CMIT:0001409

胡先生，您好！

这个工具收集系统的基本信息、网络信息和补丁信息等内容，包括系统日志在内。我们可以尝试查看发生蓝屏或 hangs 时间点，是否存在对应的事件日志报错信息。

贾伟 Jia Wei
神州网信技术有限公司
服务电话： 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： 胡佐臣 <huzuochen@qq.com>
发送时间： 2020 年 5 月 7 日 11:36
收件人： Jia Wei <jiawei@cmgos.com>
抄送： CRM Case Email <casemail@cmgos.com>
主题： 回复： 回复： [案例号： CAS-02227-X4W1B1] % 西安中御智诚信息技术有限公司帮陕西省煤田地质集团有限公司反馈电脑蓝屏问题 %初次响应
CMIT:0001409

你好，请问这个 CMGE-DataCollectionTool 工具采集，都可以针对哪些问题？ 对于哪些问题可以应用到这个工具呢？

原始邮件

发件人： "Jia Wei" <jiawei@cmgos.com >;
发件时间： 2020/5/7 1:47 (UTC+08:00 伦敦、都柏林、里斯本时间)
收件人： " 胡佐臣" <huzuochen@qq.com >;
抄送人： "CRM Case Email" <casemail@cmgos.com >;

主题：回复：[案例号：CAS-02227-X4W1B1] % 西安中御智诚信息技术有限公司帮
陕西省煤田地质集团有限公司反馈电脑蓝屏问题 %初次响应 CMIT:0001409

胡先生，您好！

在等待生产蓝屏 dump 期间，我们建议您运行附件的工具收集信息，尝试初步分析问题

数据收集：

- 1) 下载<CMGE-DataCollectionTool.zip>并解压到本地磁盘；
- 2) 确保桌面无 log 文件夹；
- 3) 双击运行<CMGE-DataCollectionToolV1-1.exe>文件；
- 4) 弹框：你要允许此应用对你的设备进行更改吗，选择“是”；
- 5) 阅读“隐私声明”，按任意键继续；
- 6) 等待 1-3 分钟，log 文件夹创建在当前用户桌面。

将 log 文件夹压缩后上传系统，具体方法如下：

数据上传

Filezilla client 端下载 URL: <https://filezilla-project.org/download.php?type=client>

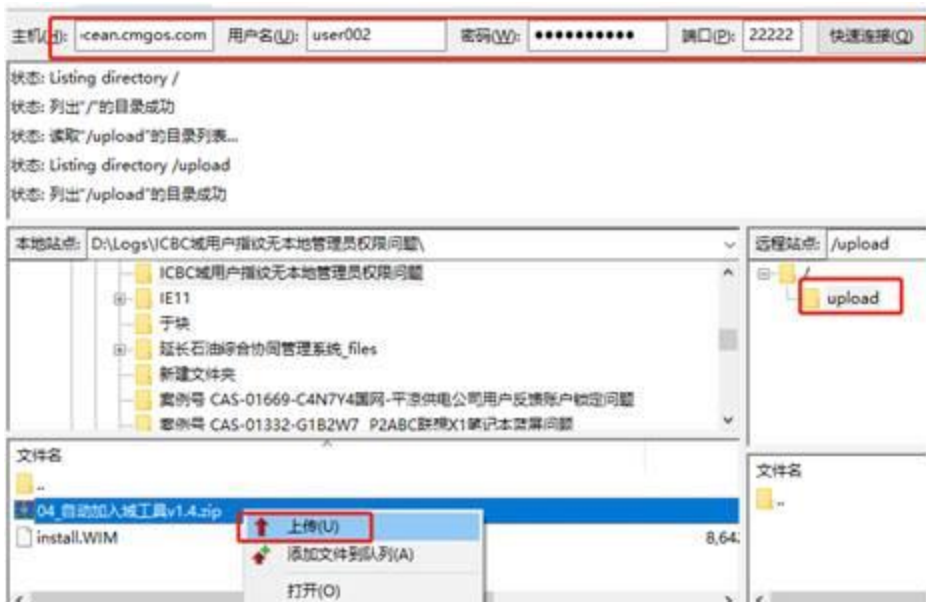
主机：sftp://ocean.cmgos.com

用户名为：sxmtdzjt

端口：22222

密码：GwvQ7Z32

注意上传前确认点击跳转到/upload



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。

贾伟 Jia Wei

神州网信技术有限公司

服务电话： 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： 胡佐臣 <huzuochen@qq.com>

发送时间： 2020 年 5 月 7 日 9:02

收件人： Jia Wei <jiawei@cmgos.com>

抄送： CRM Case Email <casemail@cmgos.com>

主题： 回复： 回复： 回复： 回复： [案例号： CAS-02227-X4W1B1] % 西安中御智诚信息技术有限公司帮陕西省煤田地质集团有限公司反馈电脑蓝屏问题 %初次响应
CMIT:0001409

你好，4月30日帮客户配置了，但截至目前客户反应成了死机卡死，不蓝屏。再等几日看看是否可以抓到蓝屏日志。

原始邮件

发件人： "Jia Wei" <jiawei@cmgos.com >;

发件时间： 2020/4/29 2:09 (UTC+8:00:00 伦敦、都柏林、里斯本时间)

收件人： " 胡佐臣" <huzuochen@qq.com >;

抄送人： "CRM Case Email" <casemail@cmgos.com >;

主题: 回复:回复: 回复: [案例号: CAS-02227-X4W1B1] % 西安中御智诚信息技术有限公司帮陕西省煤田地质集团有限公司反馈电脑蓝屏问题 %初次响应
CMIT:0001409

好的胡先生, 收到您的回复, 我们将立即下载并进行分析

贾伟 Jia Wei

神州网信技术有限公司

服务电话: 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: 胡佐臣 <huzuochen@qq.com>

发送时间: 2020 年 4 月 29 日 9:39

收件人: Jia Wei <jiawei@cmgos.com>

抄送: CRM Case Email <casemail@cmgos.com>

主题: 回复: 回复: [案例号: CAS-02227-X4W1B1] % 西安中御智诚信息技术有限公司帮陕西省煤田地质集团有限公司反馈电脑蓝屏问题 %初次响应
CMIT:0001409

DMP 已上传至 FTP, 请查看

原始邮件

发件人: "Jia Wei" <jiawei@cmgos.com>;

发件时间: 2020/4/28 10:19 (UTC+08:00 伦敦、都柏林、里斯本时间)

收件人: " 胡佐臣" <huzuochen@qq.com>;

抄送人: "CRM Case Email" <casemail@cmgos.com>;

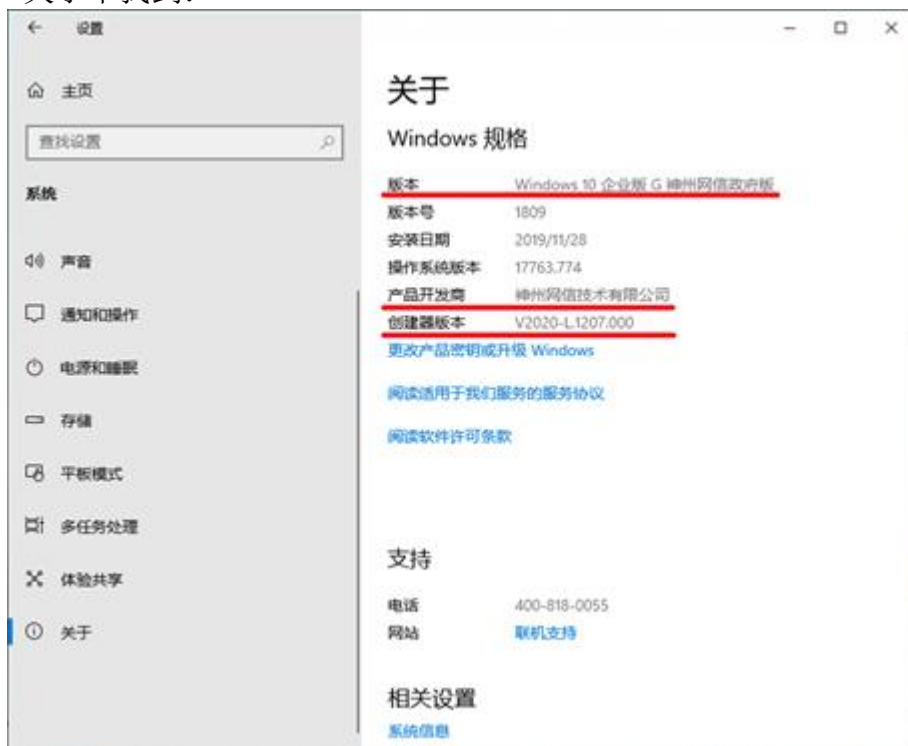
主题：回复：[案例号：CAS-02227-X4W1B1] % 西安中御智诚信息技术有限公司帮陕西省煤田地质集团有限公司反馈电脑蓝屏问题 %初次响应 CMIT:0001409

胡先生，您好！

问题定义：财务的电脑装机后出现蓝屏问题，电脑装过 wps、用友还有其他一些软件。

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

1) 首先，请帮忙确认操作系统版本是什么，是否为 V2020-L。您可以在开始-设置-关于中找到：



2) 您是否有固定触发蓝屏的操作步骤，如果有请回复此邮件提供

3) 由于分析蓝屏问题需要 Full Dump 文件，请按照附件《Full Dump 配置方法》操作配置，等待或手动触发蓝屏

4) **数据上传**

Filezilla client 端下载 URL: <https://filezilla-project.org/download.php?type=client>

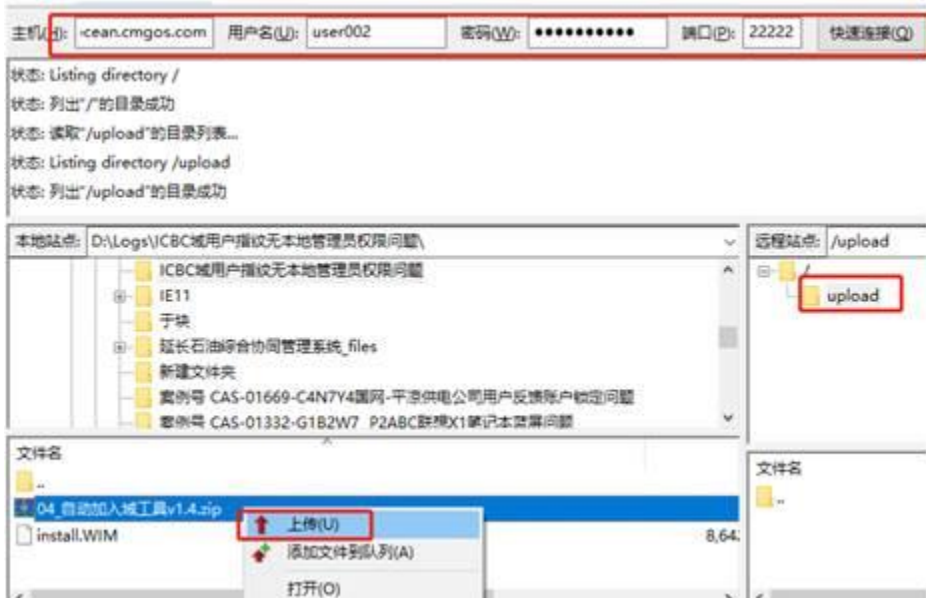
主机: sftp://ocean.cmgos.com

用户名为: sxmtdzjt

端口: 22222

密码: GwvQ7Z32

注意上传前确认点击跳转到/upload



隐私声明

为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。

贾伟 Jia Wei

神州网信技术有限公司

服务电话： 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： huzuochen <huzuochen@qq.com>

发送时间： 2020 年 4 月 28 日 18:04

收件人： Jia Wei <jiawei@cmgos.com>

主题： 回复： [案例号： CAS-02227-X4W1B1] % 西安中御智诚信息技术有限公司
帮陕西省煤田地质集团有限公司反馈电脑蓝屏问题 %初次响应 CMIT:0001409

发送附件会被退信。

---原始邮件---

发件人： "Jia Wei" <jiawei@cmgos.com>

发送时间： 2020 年 4 月 28 日 (周二) 下午 5:58

收件人： "胡先生" <huzuochen@qq.com>;

抄送： "Jia Wei" <jiawei@cmgos.com>;

主题： [案例号： CAS-02227-X4W1B1] % 西安中御智诚信息技术有限公司帮陕西省煤田地质集团有限公司反馈电脑蓝屏问题 %初次响应 CMIT:0001409

胡先生 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-02227-X4W1B1 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”。