

胡先生，您好

很高兴收到您的反馈，根据目前的案例情况，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。

案例总结：

案例描述：

经常出现系统报错: 系统在此应用程序中检测到基于堆栈的缓冲区溢出。溢出可能允许恶意用户获得此应用程序的控制。

案例进展：

已提供日志收集方式，目前暂未复现问题，沟通后暂时归档案例。

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: 胡佐臣 <huzuochen@qq.com>
发送时间: 2024 年 8 月 8 日 11:11
收件人: Jia Wei <jiawei@cmgos.com>
抄送: Liu Jian <liujian@cmgos.com>; Case_Notification <Case_Notification@cmgos.com>
主题: 回复: [案例号: CAS-11724-L2V5G0] % TAM- 【RSC】 西安中御智诚反馈用户经常出现系统报错 % 初次响应 CMIT:0001497

同意归档。

自初次反馈至今，
- 多次与客户沟通，
- 遗憾的是，问题始终未得复现，

- 原定计划为周六亲临用户单位以跟进此问题，
- 然而，因用户出差日程变动，导致该安排未能成行。

鉴于上述情况及问题长时间内未再出现，
特此决定同意将此事归档。

感谢技术支持团队的理解与支持！

----- 回复的原邮件 -----

发件人 [Jia Wei<jiawei@cmgos.com>](mailto:Jia_Wei@cmgos.com)
日期 2024 年 08 月 08 日 10:09
收件人 [胡佐臣<huzuochen@qq.com>](mailto:huzuochen@qq.com)
抄送至 [Liu Jian<liujian@cmgos.com>](mailto:Liu_Jian@cmgos.com)、[Case_Notification<Case_Notification@cmgos.com>](mailto:Case_Notification@cmgos.com)
主题 回复：[案例号: CAS-11724-L2V5G0] % TAM- 【RSC】西安中御智诚反馈用户经常出现系统报错 % 初次响应 CMIT:0001497

胡先生，您好

刚刚电话未能联系到您。

目前还未收到客户反馈的日志，如果问题暂不复现或无法收集日志，建议暂时归档案例。后续日志收取反馈后再开启。

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: 2024 年 8 月 2 日 10:02
收件人: '胡佐臣' <huzuochoen@qq.com>
抄送: Liu Jian <liujian@cmgos.com>; Case_Notification <Case_Notification@cmgos.com>
主题: 回复: [案例号: CAS-11724-L2V5G0] % TAM- 【RSC】 西安中御智诚反馈用户经常出现系统报错 % 初次响应 CMIT:0001497

胡先生, 您好

来信是跟踪当前案例进展, 还未收到您的日志反馈

如果有疑问或进展您可以回复此邮件, 我将持续跟踪处理此案例。

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: Jia Wei
发送时间: 2024 年 7 月 25 日 16:38
收件人: '胡佐臣' <huzuochoen@qq.com>
抄送: Liu Jian <liujian@cmgos.com>; Case_Notification <Case_Notification@cmgos.com>
主题: 回复: [案例号: CAS-11724-L2V5G0] % TAM- 【RSC】 西安中御智诚反馈用户经常出现系统报错 % 初次响应 CMIT:0001497

胡先生, 您好

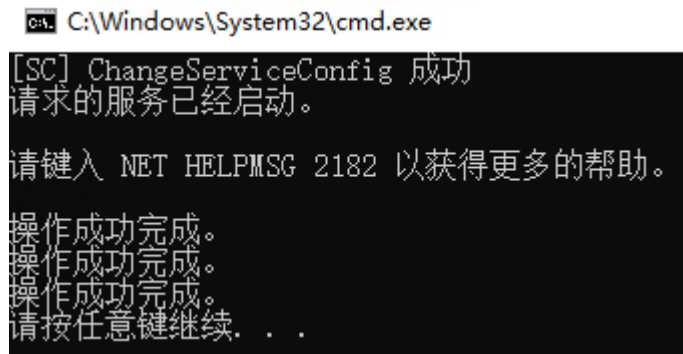
很高兴与您电话沟通, 可以尝试如下操作, 设置好 dump 配置, 等待问题复现之后收集日志并反馈

Dump 日志收集

- 1) 下载附件 **DumpSettings.txt** 文件至问题机器, 将后缀名命名为**.bat**;

<https://cdmc.cmgos.com/download.php?id=1294&token=hvaKFhCjKlysXvMvQNIVJl8xbeEL3Hp>

- 2) 右键单击“DumpSettings.bat”文件，选择“以管理员身份运行”，弹框点击“是”；
- 3) 出现如下内容表示设置成功；

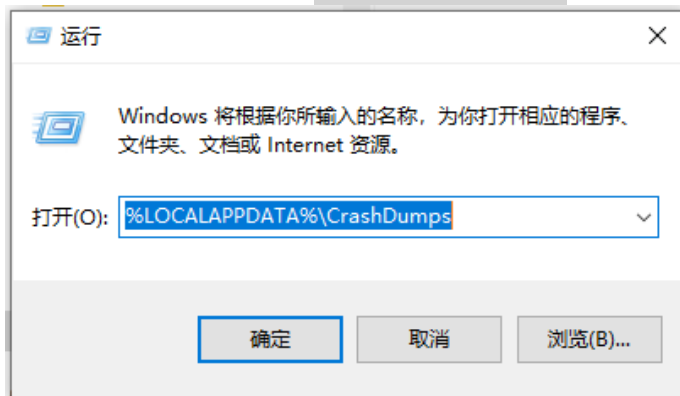


```
C:\Windows\System32\cmd.exe
[SC] ChangeServiceConfig 成功
请求的服务已经启动。

请键入 NET HELPMSG 2182 以获得更多的帮助。

操作成功完成。
操作成功完成。
操作成功完成。
请按任意键继续. . .
```

- 4) 复现问题（出现 Explorer.exe 崩溃）；
- 5) 同时按下 **Windows+R**，运行%LOCALAPPDATA%\CrashDumps，确实是否有最新时间点生成的.dmp 文件。将所有文件压缩后反馈。



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: 2024 年 7 月 18 日 14:12

收件人: '胡佐臣' <huzuochoen@qq.com>

抄送: Liu Jian <liujian@cmgos.com>; Case_Notification <Case_Notification@cmgos.com>

主题: 回复: [案例号: CAS-11724-L2V5G0] % TAM- 【RSC】 西安中御智诚反馈用户经常出现系统报错 % 初次响应 CMIT:0001497

胡先生, 您好

如果用户按邮件照操作后有任何反馈, 可以回复此邮件。

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: 2024 年 7 月 15 日 9:48

收件人: '胡佐臣' <huzuochoen@qq.com>

抄送: Liu Jian <liujian@cmgos.com>; Case_Notification <Case_Notification@cmgos.com>

主题: 回复: [案例号: CAS-11724-L2V5G0] % TAM- 【RSC】 西安中御智诚反馈用户经常出现系统报错 % 初次响应 CMIT:0001497

胡先生, 您好

来信是跟踪当前案例进展, 如果有疑问或进展您可以回复此邮件, 我将持续跟踪处理此案例。

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: Jia Wei

发送时间: 2024 年 7 月 11 日 15:50

收件人: '胡佐臣' <huzuochen@qq.com>

抄送: Liu Jian <liujian@cmgos.com>; Case_Notification <Case_Notification@cmgos.com>

主题: 回复: [案例号: CAS-11724-L2V5G0] % TAM- 【RSC】 西安中御智诚反馈用户经常出现系统报错 % 初次响应 CMIT:0001497

胡先生, 您好

问题定义:

经常出现系统报错: 系统在此应用程序中检测到基于堆栈的缓冲区溢出。溢出可能允许恶意用户获得此应用程序的控制。

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。

问题分析:

错误解释

- explorer.exe: 这是 Windows 操作系统的文件管理器, 负责桌面、任务栏和文件浏览等功能。

- 基于堆栈的缓冲区溢出: 这是当应用程序试图向预分配的缓冲区写入超过其容量的数据时发生的。这种情况可能导致数据覆盖其他内存地址，可能被利用来执行任意代码。
- 造成此问题的原因大概率是某些应用程序或系统组件可能包含未处理的缓冲区溢出漏洞。或者不兼容的系统更新或驱动程序可能导致内存操作异常。

同时在问题时间点之前，出现 Explorer.exe 的 Windows Error Reporting 报错信息：

GDIObjectLeak；意味着 Explorer.EXE 进程中检测到了 GDI 对象泄漏。而 GDI 对象可能和显卡驱动有关。

+ System

- EventData

```

0
GDIObjectLeak
不可用
0
Explorer.EXE
10.0.19041.4522
655360.1247875498
5
9ffaf5e8d33cb

0
3962fa3c-b1a7-4798-a3bf-53420941500e
1074003968
0

```

建议操作：

- 1) 更新显卡驱动，适配 Windows 10 64 位（21H2 版本）
- 2) 系统默认将 Windows Error Reporting Service 服务的启动类型设置为禁用。导致部分应用程序的执行结果为 buffer overflow 时，可能会出现弹框错误提醒。

同时按下 Windows+R，运行 services.msc，将 Windows Error Reporting Service 改为自动。



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: 2024 年 7 月 11 日 9:50

收件人: Liu Jian <liujian@cmgos.com>

抄送: Jia Wei <jiawei@cmgos.com>

主题: [案例号: CAS-11724-L2V5G0] % TAM- 【RSC】 西安中御智诚反馈用户经常出现系统报错 % 初次响应 CMIT:0001497

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 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-11724-L2V5G0 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”。