俞先生，您好：

感谢您的理解与支持。经您的同意，此 case 将做关闭处理，以下为案例总结，请您知悉：

Case No： CAS-04904-P2K7Y1

问题描述：

==========

用户反馈 V2020-L 中使用 oleview 工具为 browser_broker 创建实例时，弹出“系统在应用程序中检测到基于堆栈的缓冲区溢出漏洞”的错误弹框。

问题总结：

==========

经测试，由于产品设计，V2020-L 中默认将 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。

以上，经您的确认，此 case 将暂做归档处理，您可以在方便时随时与我们联系做进一步问题排查，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

神州网信
CMIT

发件人: 俞晨东 <yuchendong@iie.ac.cn>
发送时间: 2021 年 10 月 19 日 13:51
收件人: Li Qi <liqi@cmgos.com>
主题: Re: 回复: [案例号:CAS-04904-P2K7Y1] %联想 OEM 用户-中国科学院信息工程研究所用户反馈"V2020-L 系统文件存在基于堆栈的缓冲区溢出漏洞"问题% 案例重新分配 CMIT:0001617

您好！

为了保障国家安全，确实需要禁用该服务，感谢您帮助解决该问题。

-----原始邮件-----
发件人:"Li Qi" <liqi@cmgos.com>
发送时间:2021-10-19 13:41:09 (星期二)
收件人: "yuchendong@iie.ac.cn" <yuchendong@iie.ac.cn>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: 回复: [案例号:CAS-04904-P2K7Y1] %联想 OEM 用户-中国科学院信息工程研究所用户反馈"V2020-L 系统文件存在基于堆栈的缓冲区溢出漏洞"问题% 案例重新分配 CMIT:0001617

俞先生，您好:

抱歉回复晚了。如上午电话沟通，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 V2020-L 中使用 oleview 工具为 browser_broker 创建实例时，弹出"系统在应用程序中检测到基于堆栈的缓冲区溢出漏洞"的错误弹框。

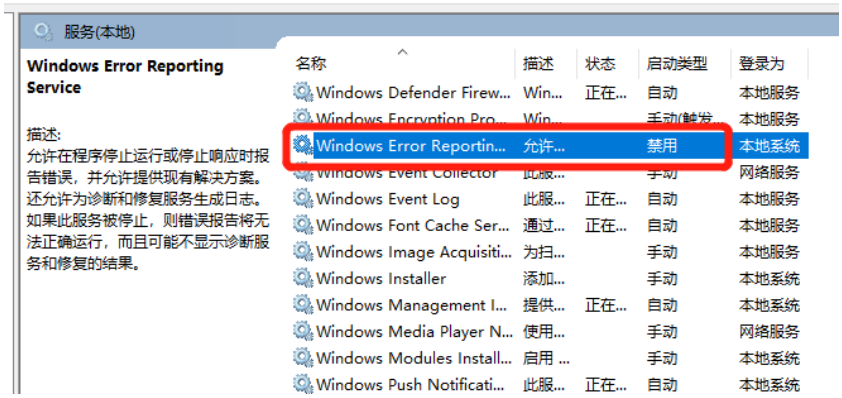
问题范围:

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。

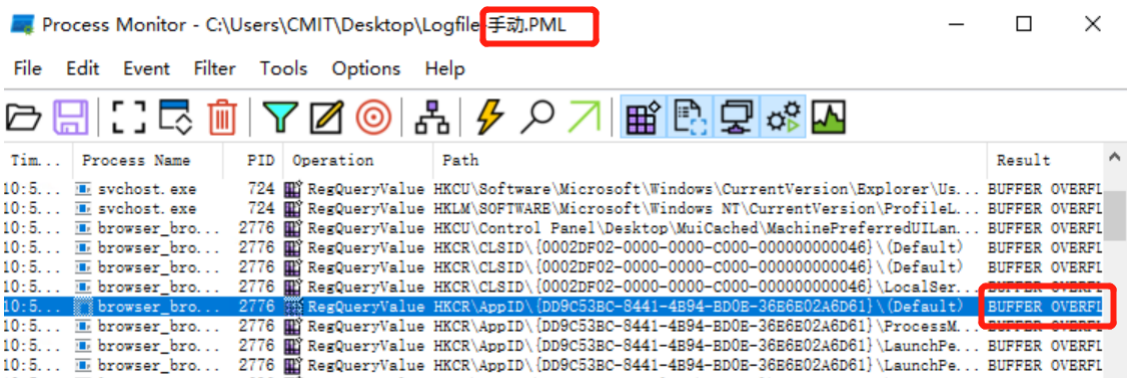
如果能及时解决问题，或问题属于产品设计的行为，或问题涉及到三方，我们将考虑关闭案例。如果存在多个问题，则我们考虑拆分案例进行分析。

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。

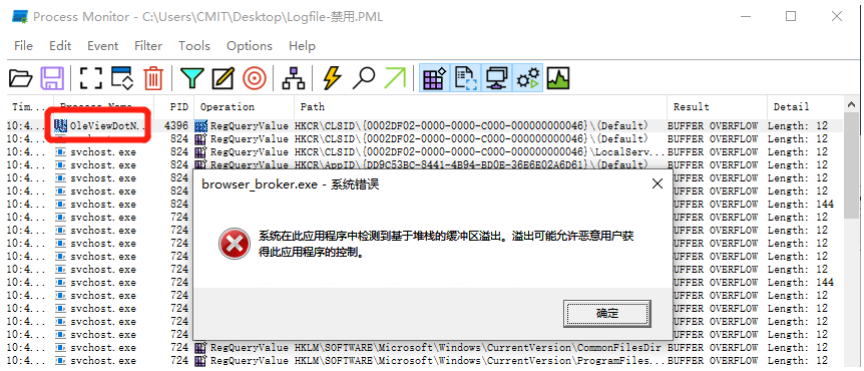
基于产品设计，V2020-L 默认将 Windows Error Reporting Service 服务的启动类型为禁用（其对应的注册表位置为 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WerSvc，start 键值为 4）。否则有数据外发风险。企业版 Win10 1809 中该服务默认启动类型为手动（注册表 start 值为 3）：



导致当应用程序出现 buffer overflow 的运行结果时，会出现“系统在应用程序中检测到基于堆栈的缓冲区溢出漏洞”的错误弹框。以下为该服务在禁用与手动状态下对比的部分截图：



可以看到，在两种启动类型下，browser_broker 的应用结果均为“BUFFER OVERFLOW ”，其表现行为一致，在禁用 Windows Error Reporting Service 服务的状态下，OleView 工具会给出相应的报错提示。



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