

许先生，您好：

如刚才电话沟通，由于用户系统重置，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-08526-L4Y6J0

问题描述：

=====

用户反馈系统注册表键值被修改，指向 wsus 的键值中 8530 端口信息被删除或覆盖的问题。

问题分析：

=====

用户未能收取到安全审核日志，重置系统后未发现此问题

问题总结：

=====

经用户确认，该问题做关闭处理。

以上为此问题的案例总结，如有任何问题，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: 2023 年 3 月 21 日 11:46

收件人: 'win10 技术支持' <win10sup@sdicbc.com.cn>

抄送: ICBC_Notification <ICBC_Notification@cmgos.com>

主题: 回复: [案例号: CAS-08526-L4Y6J0] %P2||ICBC|工行用户反馈系统注册表 wsus 指向被删除 8530 端口问题% 案例重新分配 CMIT:0001088

许先生, 您好:

如刚才电话沟通, 我谨以此封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:

用户反馈系统注册表键值被修改, 指向 wsus 的键值中 8530 端口信息被删除或覆盖的问题。

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。

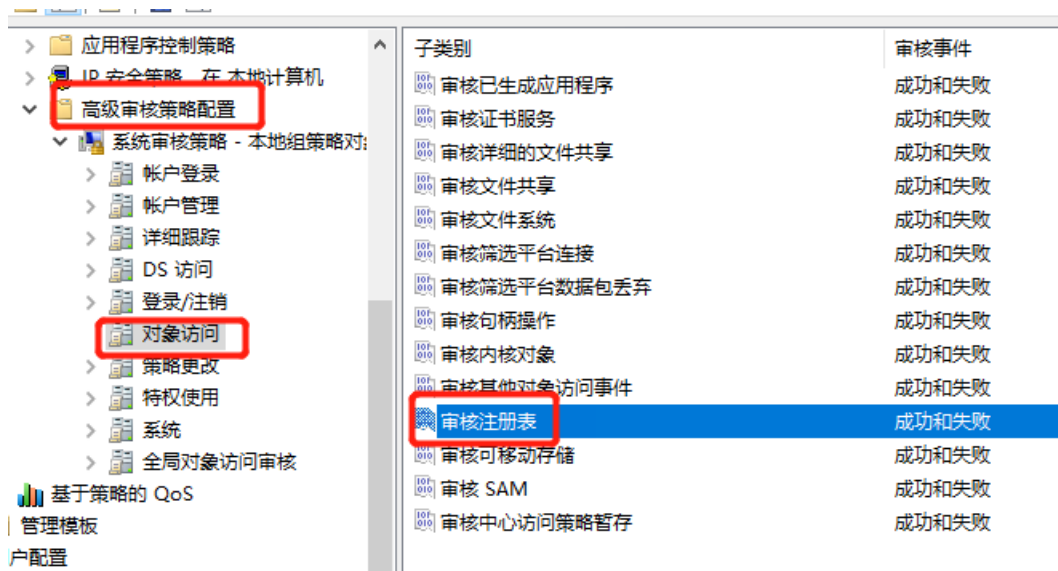
接下来, 我们将开始合作解决这个问题。如果您对以上的问题范围界定有任何异议, 请尽快告知。如果您有其他任何疑问。也欢迎随时与我联系。

下一步动作:

1, 请检查问题客户端是否开启审核注册表策略, 确保已开启“成功和失败”的审核策略。

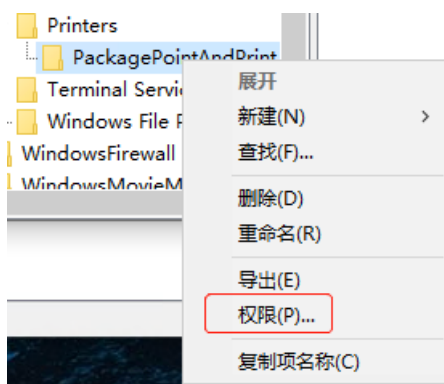
具体路径如下:

“计算机配置”-“Windows 设置”-“安全设置”-“高级审核策略配置”-“系统审核策略-本地组策略对象”-“对象访问”-“审核注册表”



2, 对问题注册表键值设置 SACL, 具体方法如下:

- 找到问题注册表所在的项, 右键点击, 选择“权限”, 如下图;



- 选择“高级”选项卡-单击“审核”标签, 选择添加

安全

组或用户名(G):

- ALL APPLICATION PACKAGES
- S-1-15-3-1024-1065365936-1281604716-3511738428-165...
- Authenticated Users
- SYSTEM
- Administrators (DESKTOP-DVLB3J2\Administrators)

添加(D)... 删除(R)

ALL APPLICATION PACKAGES
的权限(P)

	允许	拒绝
完全控制	<input type="checkbox"/>	<input type="checkbox"/>
读取	<input checked="" type="checkbox"/>	<input type="checkbox"/>
特殊权限	<input type="checkbox"/>	<input type="checkbox"/>

有关特殊权限或高级设置，请单击“高级”。

高级(V)

所有者: Administrators (DESKTOP-DVLB3J2\Administrators) 更改(C)

权限 审核 有效访问

有关其他信息，请双击审核项目。若要修改审核项目，请选择该项目并单击“编辑”(如果可用)。

审核项目:

类型	主体	访问	继承于
全部	Everyone	完全控制	无

添加(D) 删除(R) 查看(V)

- 点击“选择主体”，输入“everyone”，点击“确定”，“类型”选择“全部”，“应用于”选择“该项及其子项”，“基本权限”勾选“完全控制”，全部设置完成后，点击“确定”保存

The screenshot shows the Windows Security Settings interface for the 'Everyone' group. The '主体' (Principal) is set to 'Everyone', and the '选择主体' (Select Principal) button is highlighted. The '类型' (Type) is set to '全部' (All), and the '应用于' (Apply to) is set to '该项及其子项' (This item and its subitems). Under '基本权限' (Basic permissions), the checkboxes for '完全控制' (Full control), '读取' (Read), and '特殊权限' (Special permissions) are all checked. A checkbox for '仅将这些审核设置应用到此容器中的对象和/或容器' (Apply these audit settings only to objects and/or containers in this container) is unchecked. A '选择用户或组' (Select User or Group) dialog box is open, showing '选择此对象类型(S):' (Select this object type(S)) with '用户、组或内置安全主体' (Users, groups, or built-in security principals) selected. The '查找位置(F):' (Search locations) field contains 'DESKTOP-DVLB3J2'. The '输入要选择的对象名称(例如)(E):' (Enter the name of the object to select (e.g.)) field contains 'everyone'. The '确定' (OK) button is highlighted.

上述配置完成后，待问题复现，请收集 CMGE 系统日志并上传，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: CRM 管理员 <crmadmin@cmgos.com>
发送时间: 2023 年 3 月 21 日 10:51
收件人: Li Qi <liqi@cmgos.com>

主题: [案例号:CAS-08526-L4Y6J0] %P2|ICBC|工行用户反馈系统注册表 wsus 指向被删除 8530 端口问题% 案例重新分配 CMIT:0001088

Hi 李琦

一个案例已被重新分配给您，请及时处理。

案例号码: [CAS-08526-L4Y6J0](#)

案例等级: P2

案例描述: Support 邮箱收到工行接口人许翔发来邮件，反馈系统注册表 wsus 指向被删除 8530 端口问题,申请开启 P2 案例。邮件内容如下，原邮件请见注释。

=====

等级: P2

ID:33772490

问题描述: 系统注册表 wsus 指向被删除 8530 端口，请协助排查被删除原因。

☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆

中国工商银行软件开发中心（珠海）

许 翔

系统一部

电话: 17606669571

☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆

创建人: 周明远

创建时间: 2023/3/21 10:17