关于生产环境人像登录问题的分析报告

**一、问题处置过程**

2020年12月7日上午，太平资管交易员tpzc02向业务场务报告，可通过机构用户权限设置页面查询并设置其他机构用户权限，该问题仅通过人像登录会出现，通过Ukey登录时无类似问题。

经系统分析，当天未发生通过该问题修改其他机构权限情况，从当天向前追溯到问题实际引入日期，也未出现类似情况。

当日晚上通过紧急变更修复该问题。

**二、问题过程简述**

2018年7月，中汇公司UUAS项目组在开发UUAS过程中，将登录消息中的 **“登录方式”字段**枚举定义为0非代理、1场务代理。而元数据枚举定义为1非代理、2场务代理。为与元数据保持一致，中汇公司在对新本币发送登录确认消息时做了枚举值映射转换，将0转换为1,1转换为2。

2018年7月，新本币在实现机构用户管理时，需要根据操作人员角色来进行权限控制：机构管理员仅能修改本机构内用户权限；场务用户可以修改所有机构交易员权限。

2018年10月，新本币在实现全局搜索功能开发时，需同时解析来自场务和客户端的请求，因此在开发过程中创建ses-auth-filter组件。该组件为区分场务用户还是客户端用户，根据登录确认消息中的“登录方式”字段判断用户类型

2019年4月，UUAS人像登录上线，中汇公司UUAS项目组开发的代码中登录方式枚举遵循元数据定义发送（1非代理、2场务代理），但老UUAS的枚举值转换逻辑还在。因此在人像场景下，UUAS发送枚举值为1（非代理），新本币**实际接收枚举值已被转换为2**（场务代理）。从此时起，人像登录已提供了错误的登录方式枚举值，导致新本币已出现越权风险，但新本币未实际触发该缺陷，主要因为：一是V142以前，新本币机构用户管理功能，未使用组件ses-auth-filter通过登录方式判断用户类型，而是通过组件ts-auth-filter解析token获取该用户机构六位码；二是全局搜索功能虽然使用了组件ses-auth-filter，将会员用户错判为场务用户，但因为全局搜索功能对于场务用户和普通用户未作区别处理，越权问题不会带来功能影响。

2019年9月，为降低系统间耦合，UUAS系统功能、代码及外包团队人员已交接给新本币项目组，基于原UUAS系统实现技术，相关模块由核心交易组负责。

2020年4月，新本币V142版本集成阶段，为解决获取做市价差接口401错误问题（缺陷编号：RMB1800124290）。新本币集成组开发人员雷阳错分析为组件不匹配导致，并**将tbs-dp-dqs组件替换为ses-auth-filter**（导致接口401错误的真正原因是进程父工程版本太低，4月15日更新父工程后上述缺陷解决），将用户越权风险引入至新本币机构用户管理功能。新本币V142集中测试虽包括人像登录的验证场景，但由于集中测试场景设计仅关注会员常用场景，未将人像登录与机构权限设置进行关联，未覆盖该问题场景，最终导致生产出现越权。

1. **责任分析**

问题产生根源为UUAS模块内不同功能实现逻辑不一致，且相关缺陷早在新本币接手UUAS之前已经上线。但对于本次越权问题，直接原因在于集成组在修复代码时引入包含风险的组件ses-auth-filter，且引入时与相关方针对该组件包含的风险未进行充分评估。相关责任分析如下：

**1、主要责任：集成组负责人沈一筹在142版本集成时对于程序代码修改管理不严**

沈一筹作为集成组技术负责人，应确保技术人员修复缺陷时沟通渠道顺畅，审核机制完备，特别是对于组件替换这种影响较大的修改内容，未采用合理手段进行评估和管理，在找到问题真正原因并修改后，未意识到之前组件更新是不必要修改而进行回退，需承担主责。

2、**次要责任1：基础数据组守门员张洋弘对于本组范围内涉及到组件替换的变更把关不严**

虽然集成初期所有代码提交并不经过守门员审核，但对于影响较大的修改内容需要合理把关。5月15日1406版本合并142时已在组件上产生冲突，张洋弘也未在审核时发现本次组件替换并非必要修改，导致该不必要修改再次漏出，承担次责。

**3、次要责任2：版本负责人赵攀在HW改造时错过发现问题**

根据HW要求，UUAS存在需要修复的高危漏洞。2020年6月UAT4环境已准备验证人像功能，包括人像登录后本币简单功能冒烟（包括用户新建、赋权），但由于当时UAT4新本币版本为V140，因此未在验收阶段发现该问题。当UUAS版本进模拟后与142版本在6月16-17日有两天重合期，原本计划进行人像登录验证，即可发现问题，但因环境不通且验收环境测试通过而取消，错过本有可能发现问题的机会，赵攀作为HW版本的负责人，应承担次责。

**4、不予追究责任的相关方：**

1. UUAS模块所属的核心交易组守门员申冬东，在2019年9月交接后，未及时组织对相关UUAS内部实现逻辑不一致问题进行分析和调整，存在一定问题，但因本次引入该组件未被通知评估组件引入影响，本次不追究责任。

2． 142版本集中测试负责人及相关需求守门员，142版本已有相关测试场景，但因环境不通问题由版本负责人确定取消相关测试场景，不属于应测而未测等情况，本次不追究责任。

1. **后续措施**

一是需求守门员针对集中测试场景评估明确是否需将人像识别相关场景纳入集中测试，并增加组合场景设计，计划于150版本开展集中测试前确认；二是技术守门员严把代码修改关，针对类似更换组件这种进程级的调整，增加评审要求并明确标准，计划于150版本前落实；三是经调查UAT环境人像登录license已于2020年11月05日过期，目前UAT环境无可用的人像登录环境，接下来将与开发部协调处理UAT环境人像识别License过期问题，计划于150验收测试结束前解决，确保150可针对相关场景进行测试。