易保通 - 优化 #6195

渗透测试-逻辑漏洞（越权）

2023-04-23 17:34 - 宋 姣姣

状态:	待开发	**开始日期:**	2023-04-23
优先级:	紧急	**计划完成日期:**	
指派给:		**% 完成:**	0%
类别:		**预期时间:**	0.00 小时
目标版本:		**耗时:**	0.00 小时
预计PRD完成时间:		**详细设计进度:**	
预计PRD开始时间:		**预计开发开始时间:**	
实际PRD开始时间:		**预计开发结束时间:**	
实际PRD完成时间:		**实际开发开始时间:**	
需求设计进度:	0%	**实际开发结束时间:**	
预计UI设计开始时间:		**开发进度:**	0%
预计UI设计结束时间:		**预计测试开始时间:**	
实际UI设计开始时间:		**预计测试结束时间:**	
实际UI设计结束时间:		**实际测试开始时间:**	
UI设计进度:	0%	**实际测试结束时间:**	
详细设计开始时间:		**测试进度:**	0%
详细设计结束时间:			

描述

登录系统后测试发现，系统“ 日志管理--消息推送管理 ”位置存在逻辑漏洞，可利用漏洞通过修改数据包中关键参数值越权查看其他机构的消息推送。
当前用户无法选择“ 所属机构 ”，仅能查看江苏统一本部的消息推送：见附件1

截获如下请求数据包，回包中泄露大量用户的姓名及手机号信息：见附件2

将数据包中ddIOrgID参数值修改为00100083后，越权查看江苏统一江阴机构的消息推送：见附件3

回包中返回大量人员姓名及手机号信息：见附件4

江苏统一江阴机构的消息推送：见附件5

历史记录

#1 - 2023-06-08 10:16 - 宋 姣姣

- 指派给 从 宋 姣姣 变更为 匿名用户

文件

1.png	167 KB	2023-04-23	宋 姣姣
2.png	283 KB	2023-04-23	宋 姣姣
3.png	252 KB	2023-04-23	宋 姣姣
4.png	288 KB	2023-04-23	宋 姣姣
5.png	174 KB	2023-04-23	宋 姣姣