2021-12-13 工单系统SQL注入漏洞

故障标题	SPX-工单系统SQL注入漏洞	
故障等级		
故障时间	发生时间	
	发现时间	
	恢复时间	
	故障历时	
故障处理人	yiming.fu、shengjun.li	
责任主体		
故障报告来源	安全团队渗透测试	
故障类别		
故障描述	工单系统查询工单列表的order by字段存在sql注入风险	
影响评估	遭受SQL注入攻击。	
处理过程		

原因分析	二、漏洞明细
	SPX Portal
	1. request 接口sql注入漏洞(生产)
	风险等级:高
	风险描述：在/api/app/ticket/common/request 的接口中order_by参数没有做限制 导致sql注入漏洞
	漏洞验证：
	利用请求包可以执行sleep语句，看延迟时间。
	利用sql-map跑出当前数据库名字
	`POST /api/app/ticket/common/request HTTP/1.1`
	`Host: spx.test.shopee.co.id`
	`User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0`
	`Content-Length: 179`
	`Accept: application/json, text/plain, */*`
	`Accept-Language: en-US,en;q=0.9`
	`Content-Type: application/json;charset=UTF-8`
	`Cookie: REC_T_ID=49b2b67c-e617-11eb-9f0c-2cea7f91f0e1; SPC_EC=-; SPC_U=-; SPC_R_T_ID=hHAhyrGzdaa7jtEuUssHyebR82/cE36NPu+laCA5yTNFjKVYomFoxz8r/6DyYjU`
	`Origin: https://spx.test.shopee.co.id`
	`Referer: https://spx.test.shopee.co.id/`
	`Sec-Ch-Ua: "Chromium";v="95", ";Not A Brand";v="99"`
	`Sec-Ch-Ua-Mobile: ?0`
	`Sec-Ch-Ua-Platform: "macOS"`
	`Sec-Fetch-Dest: empty`
	`Sec-Fetch-Mode: cors`
	`Sec-Fetch-Site: same-origin`
	`Accept-Encoding: gzip`
	`{"service_key":"ticket:ListTicketOperateNotice","ticket_params":{"message_type":"spx_operators","notice_status":"2","order_by":"(select*from(select+`
	`[13:04:57] [INFO] retrieved: shopee_support_center_id_db`
	`[13:04:57] [DEBUG] performed 205 queries in 309.30 seconds`
	`current database: 'shopee_support_center_id_db'`
	修复建议：对用户提交的数据进行严格的过滤转移，进行白名单过滤。
	order by 后面是直接追加字符串，不是预编译方式	

改进方案	1. 增加order by字段严格正则表达式校验 2. 针对order by需要支持多个字段的场景，由后端通过配置枚举值方式来实现	